



会議

改訂日：2019年2月19日

この章では、企業展開におけるビデオおよび音声会議のコンポーネントと導入方法について説明します。また、会議のアーキテクチャーについて説明し、会議の導入プロセスに含まれる主なタスクについて概要を示します。

会議の導入プロセスの主なタスクはそれぞれ、そのタスクに必要な手順をリストする「概要」セクションから始まり、そのタスクの重要な「導入上の考慮事項」を扱うセクションが続きます。その後、「概要」セクションでリストされた導入タスク（展開タスク）の詳細を示すセクションが続きます。

この章の新規情報とは

C:表 3-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

C:表 3-1 新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Meeting 管理	この章の各項で説明	2019年1月23日
会議参加者の最大数	会議ソリューションのスケールリング (C: 3-15 ページ)	2017年8月30日

コア コンポーネント

コア アーキテクチャには、以下の主要な会議要素が含まれます。

- 音声 / ビデオ会議と会議リソース管理用の Cisco Meeting Server
- 会議のプロビジョニング、モニタリング、およびスケジューリング用の Cisco TelePresence Management Suite (TMS)
- Microsoft Exchange のルームおよびリソース カレンダーとインターフェイスするための Cisco TelePresence Management Suite Extension for Microsoft Exchange (TMSXE)
- Cisco Meeting Management の会議のモニタリングと管理

加えて、Cisco TMS アーキテクチャには、次のシスコ以外のコンポーネントが含まれています。

- Microsoft SQL データベース
- Microsoft Active Directory
- Microsoft Exchange or Microsoft Office 365
- ネットワークロードバランサ

主なメリット

- すべてのデバイス タイプでの会議ユーザ エクスペリエンスが簡略化および最適化されました
- 無期限、スケジュール、インスタントのいずれかまたはすべての会議の 1 つ以上のリソースの導入をサポートする柔軟性と拡張性のあるアーキテクチャ
- 会議リソースとプロセスの高可用性
- ビデオ ネットワークでの復元性
- ホストで会議の参加者と会議室をスケジュールするための単一のツール
- マルチパーティ ライセンスは、ブリッジ上のすべての会議リソースへのフル アクセスを可能にします
- 1 つのインターフェイスで会議をモニタおよび管理する White Glove サービス

会議タイプ

会議ソリューションは、C : 表 3-2 に示す会議タイプと会議機能をサポートします。

C : 表 3-2 会議の種類

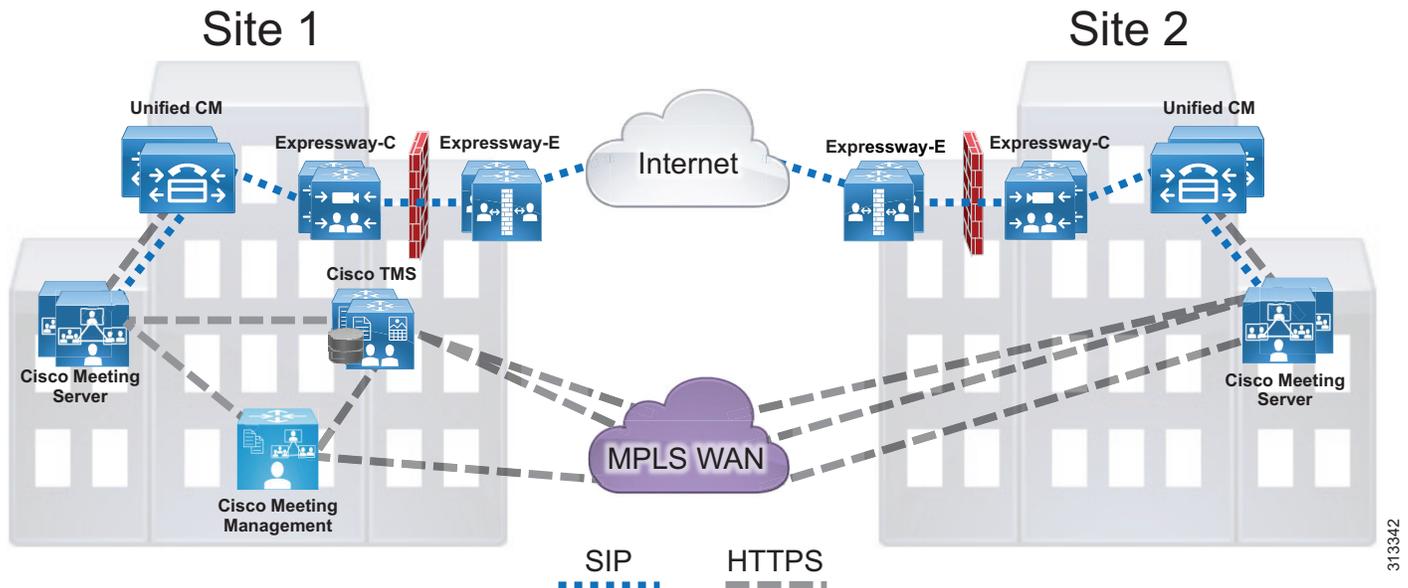
会議タイプ	説明
[インスタント会議 (Instant conferences)]	Unified CM でホストされたポイントツーポイント コールから、会議ブリッジにホストされた三者コールへのエスカレートは手動で行います (アドホック会議とも呼ばれます)。インスタント会議は、会議前にスケジュールまたは用意されません。
[無期限の会議 (Permanent conferences)]	事前のスケジュールなしで会議を行えるようにする、事前定義されたアドレス。会議ホストはその他のユーザとアドレスを共有します。それらのユーザは、いつでもそのアドレスにコールインできます (ミーティング会議、スタティック会議、または、ランデブー会議とも呼ばれます)。この章で説明する無期限会議では、Cisco Meeting Server スペースが使用されます。スペースをユーザベースにすることができ、会議名、レイアウト、PIN などの項目に関して Cisco Meeting Server からスペースがプロビジョニングされます。スペースを作成する方法として、ユーザのインポート、API、または手動作成が可能です。
スケジュール済み会議	開始および終了時間のある (オプションで一連の参加者を事前定義する)、Cisco TMS を介して、または Cisco TMS を使用した統合、あるいはその両方を使用して予約する会議。

アーキテクチャー

会議アーキテクチャは、ブリッジ リソース用およびリソース管理用の Cisco Meeting Server、リソースのプロビジョニング、スケジュールリング用の Cisco TelePresence Management Suite (TMS)、会議モニタリング用の Cisco Meeting Management、およびコール処理用の Cisco Unified Communications Manager (Unified CM) で構成されます。このアーキテクチャでは SIP コール制御が排他的に使用されます。すべての会議タイプ用の会議ブリッジとして Cisco Meeting Server を使用し、SIP トランクを使用して Cisco Meeting Server を Unified CM に接続します (C : 図 3-1)。

Unified CM は、HTTPS 経由で XML-RPC を使用して Cisco Meeting Server と通信し、インスタント会議用の会議ブリッジを制御します。Cisco TMS は REST API 接続を使用して Cisco Meeting Server にリンクし、会議リソースのプロビジョニングとスケジュールリングを行います。Cisco Meeting Management および Cisco Meeting Server は、REST API、イベントサブスクリプション、およびコール詳細レコード (CDR) インターフェイスを介して接続されて、会議管理機能を実行します。また、Cisco Meeting Management は、TMS Booking API を使用して Cisco TMS に接続し、スケジュールされた会議を管理します。(C : 図 3-1)。

C : 図 3-1 アーキテクチャの概要

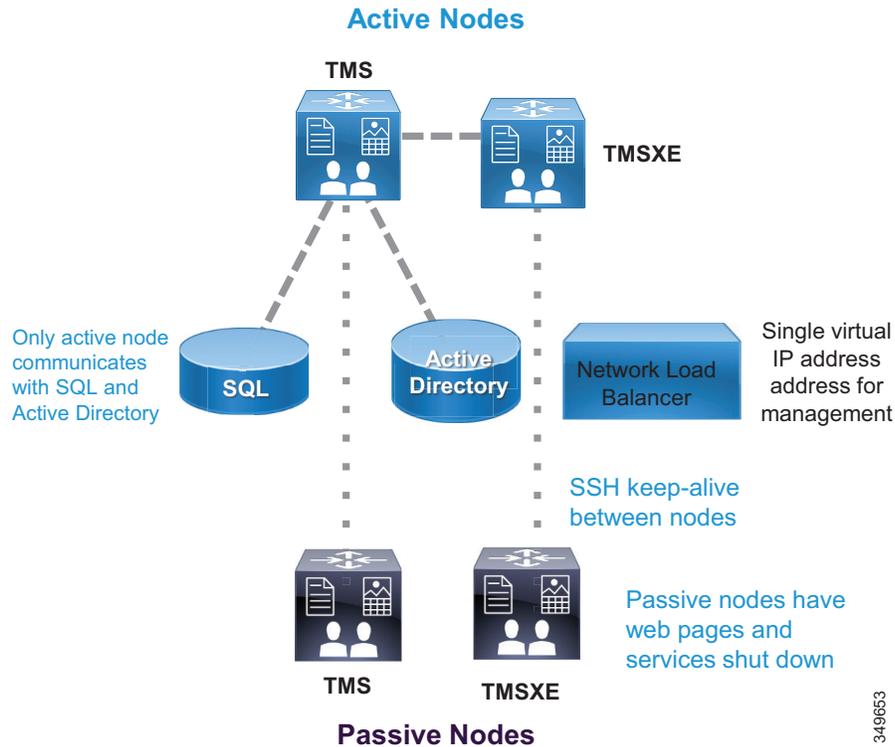


313342

ライセンスに関しては、各 Cisco Meeting Server にマルチパーティ ライセンスをインストールして、他の機能ライセンスと一緒に使用します。デフォルトで、システム内のすべてのユーザが Shared Multiparty Plus (SMP+) を使用します。また、Personal Multiparty Plus (PMP) が必要な場合は、Cisco Meeting Server API 経由で PMP+ をユーザに割り当てる必要があります。

スケジューリング アーキテクチャは、Cisco TMS および TMSXE 両方のアクティブ ノードとパッシブ ノードで構成されています。これらは、ネットワーク ロード バランサの後ろに導入されています。アクティブ ノードは着信要求を処理します。一方、パッシブ ノードはスタンバイ モードで動作し、その Web ページとサービスがロック ダウン状態になってすべての着信トラフィックを拒否します。大規模な Cisco TMS 展開 (サイジングの章を参照) では、C : 図 3-2 に示すように、Cisco TMS と TMSXE を別々の仮想マシンにインストールする必要があります。TMS サーバは顧客データ センターに設置され、そこでは組織の SQL 展開もホストされます。すべてのサーバ ノードが、外部の Microsoft SQL データベースから機能します。加えて、会議を適切にスケジュールするにはエンドポイント、Cisco Meeting Server、および Unified CM が使用されます。(C : 図 3-2)。

C : 図 3-2 スケジューリング アーキテクチャの概要



Cisco Meeting Management は Cisco Meeting Server の外部にある別個のサーバ上で、Cisco Meeting Server 導入環境専用として稼働します。Cisco Meeting Management ユーザは、ユーザ認証とユーザ ロールの判別に使用される LDAP ディレクトリ内にあります。Cisco Meeting Management は、イベント サブスクリプション インターフェイスと REST API を使用して、Cisco Meeting Server で会議管理機能を実行します。Cisco Meeting Management は Cisco Meeting Server 上の CDR 受信者として自己設定して、コール関連のイベントを受信します。これにより、会議がいつ開始したか、または終了したのかという情報や、その他のコール アクティビティが認識されます。Cisco Meeting Management は、Cisco TMS 用 Booking API を使用して、Cisco TMS から今後予定されている会議の情報を取得します。(C : 図 3-3)。

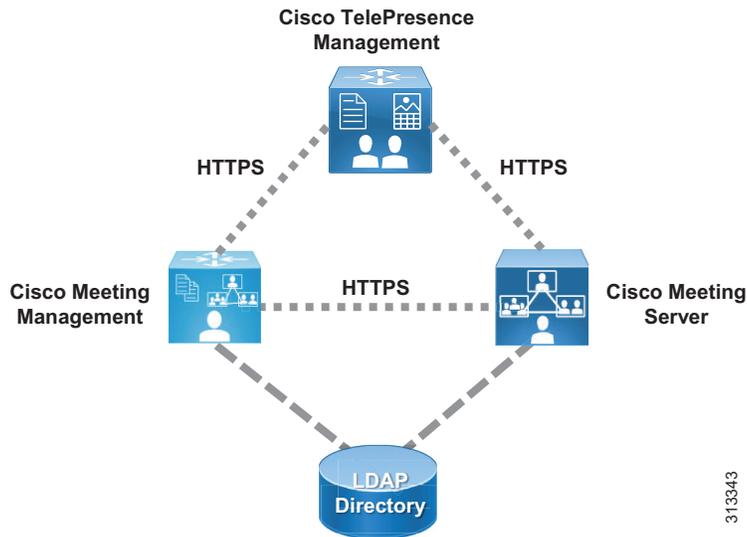
Cisco Meeting Server と TMS の互換性のあるバージョンについては、以下で入手できる最新バージョンの *Cisco Meeting Management* インストールおよび設定ガイドを参照してください。

<https://www.cisco.com/c/en/us/support/conferencing/meeting-management/products-installation-guides-list.html>


注

Cisco Meeting Management には、適切なライセンスを持つ Cisco Meeting Server インスタンス以外の追加ライセンスは必要ありません。

C : 図 3-3 Cisco Meeting Management のアーキテクチャ

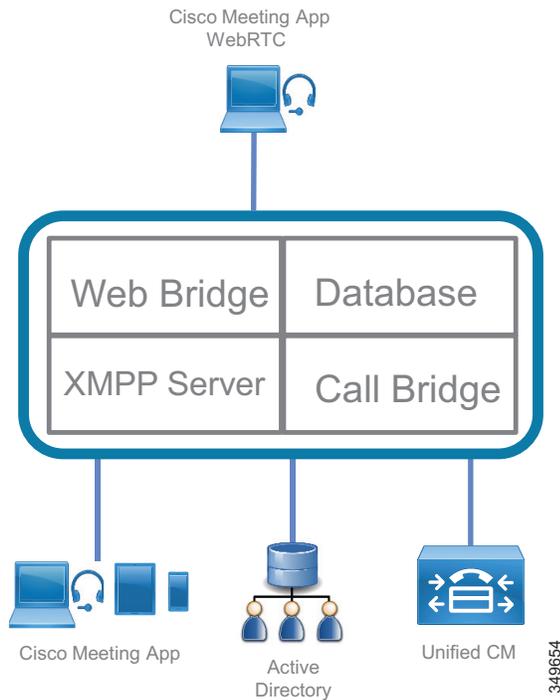


313343

Cisco Meeting Server の役割

Cisco Meeting Server は、ビデオ会議機能 (C : 図 3-4) を提供してすべてのタイプの会議を処理できる複数のコンポーネントで構成されます。Call Bridge コンポーネントは、コール制御用の Unified CM と統合し、会議機能を実行するためのリソースを提供します。すべての Cisco Meeting Server 会議がスペース上でホストされます。スペースは、音声、ビデオ、コンテンツ共有機能を備えた、スペース URI またはディレクトリ番号を使ってアクセス可能な仮想会議室です。Cisco Meeting Server は、ユーザをシステムにインポートするために Microsoft Active Directory などのディレクトリ サーバと統合する必要があります。インポートプロセス中に、フィールド マッピング 表現設定を使用してスペースが作成されます。ユーザとスペースに関するすべての情報がデータベースに保存されます。参加者は、シスコまたはサードパーティ製の標準的なビデオ エンドポイント、Cisco Jabber クライアント、または Cisco ミーティング アプリを使用して会議に参加できます。XMPP サーバは、Cisco ミーティング アプリ経由でログインするユーザを認証します。ログイン後に、Web Bridge が WebRTC クライアント ユーザを Call Bridge に接続します。

C : 図 3-4 Cisco Meeting Server 内部のコンポーネント



注 すべての Cisco Meeting Server コンポーネントが C : 図 3-4 に表示されているわけではなく、エンタープライズ コラボレーション プリファード アーキテクチャに関連したコンポーネントのみが表示されています。

Cisco ミーティング アプリは Cisco Meeting Server のクライアントであり、ネイティブ デスクトップまたはモバイル アプリケーションとして、あるいは WebRTC ブラウザ アプリケーションとして使用可能です。Cisco ミーティング アプリを使用すれば、ユーザは音声、ビデオ、およびコンテンツ共有を使用する会議にログインし、参加することができます。WebRTC クライアントを使用すれば、Cisco Meeting Server アカウントを持っていないユーザがゲストとして会議に参加することができます。加えて、Cisco ミーティング アプリを使用するとユーザは会議を開催したり、参加者の表示 / ミュート / 削除などの操作を実行したり、録音を開始 / 停止したり、独自のスペースを作成して編集することができます。



注 Cisco ミーティング アプリをエンタープライズ ネットワークの内側と外側のどちらにも展開して会議に参加させることができますが、このエンタープライズ コラボレーション プリファード アーキテクチャではエンタープライズ ネットワーク内部の展開のみを扱います。エンタープライズ ネットワークの外側の展開については、<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html> にある Cisco Meeting Server 構成ガイドの最新版を参照してください。

会議用の Cisco Meeting Server を使用すると、次のようなメリットがあります。

- 小規模な展開と大規模な展開のどちらにも簡単にスケーリングし、必要に応じてキャパシティを段階的に追加できる
- すべてのデバイス タイプで簡略化された、直感的かつ最適な会議エクスペリエンス
- マルチパーティ ライセンスを使用すると、利用可能な基盤ハードウェアの上限に達するまで会議の参加人数を増やすことができる
- 1 つの展開モデルですべての会議タイプに対応

Cisco TMS の役割

Cisco TMS は、会議スケジューリングと会議室システム予約を提供します。Unified CM はエンドポイントの設定管理を維持し、TMS はカレンダー情報をこれらのエンドポイントに配信できます。管理者は、組織のデフォルト会議のパラメータを設定できます。パラメータの設定後に、このテンプレートに基づいて個々の会議が作成されます。

TMS 機能の一部（電話帳、ソフトウェア管理、レポート機能など）はプリファードアーキテクチャで使用されません。

Microsoft Exchange に対する Cisco TMS Extension の役割

エンドユーザが複数の会議室リソースを使用する会議を Microsoft Outlook でスケジュールすると、Exchange の Exchange Web Service (EWS) 機能により、そのイベントが TMS にスケジュール済み会議として同期されます。この同期は双方向であるため、管理者またはサポート担当員が、会議主催者の Outlook イベントにアクセスせずに、会議を更新できます。組織内で会議に使用する予定のすべてのエンドポイント リソースが、1 つの Exchange 会議要求にリストされている必要があります。

Cisco Meeting Management の役割

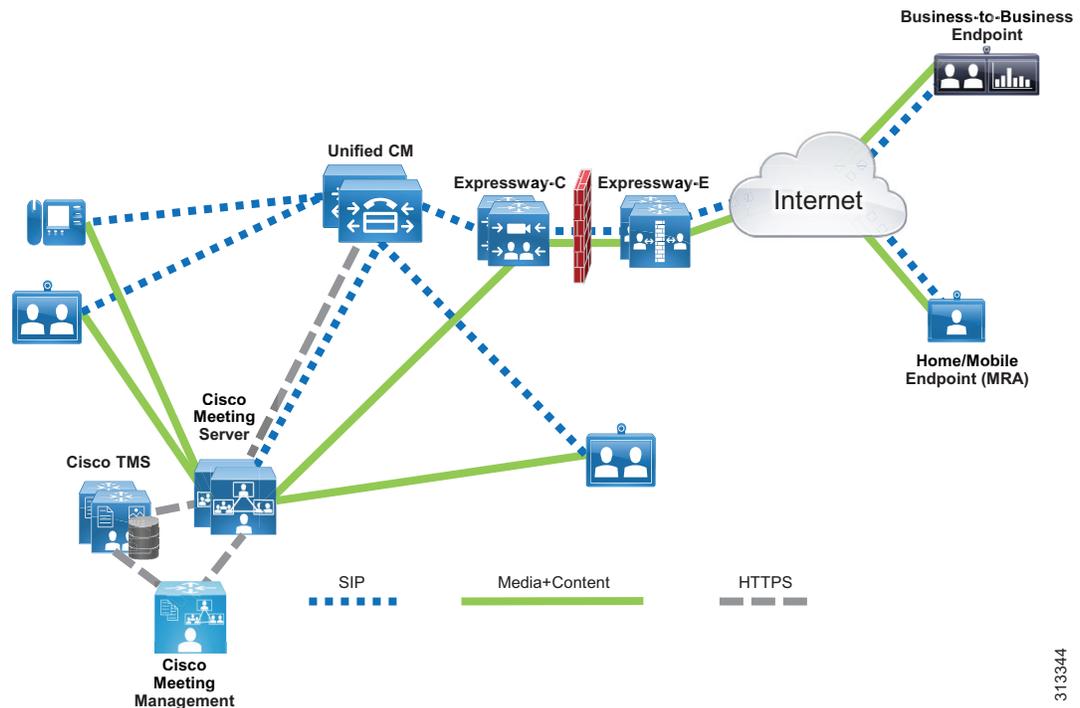
Cisco Meeting Management は Cisco TMS と併せて使用することで、Cisco Meeting Server に完全な管理機能を提供します。Meeting Management では、顧客に White Glove サービスを提供することができます。また、オペレータに、アクティブな会議、過去の会議（最長 7 日前）、または今後の会議（最長 24 時間前）の一覧を表示します。さらに、オペレータは、参加者、会議の期間、会議の開始時刻など、個々の会議に関する詳細情報を表示することができます。会議中、オペレータは、録音またはストリーミングの開始または停止、レイアウトの変更、参加者の追加またはドロップ、会議の終了などの会議管理機能を実行し、アクティブな発言者を確認することができます。個々の参加者レベルでは、オペレータは音声またはビデオのミュート・ミュート解除、レイアウトの変更、重要度の設定・設定解除、あるいは参加者の通話統計を確認することができます。

Cisco Meeting Management のユーザは、管理者、またはビデオ オペレータのいずれかのユーザグループに属します。各ユーザグループは、ユーザが割り当てられているディレクトリ内で定義される LDAP グループにマッピングされます。ユーザがポータルにログインすると、会議管理はディレクトリを使用してユーザを認証し、グループのメンバーシップを判断します。管理者は、Cisco Meeting Management ポータルのすべての機能へのフル アクセス権を持っています。ビデオ オペレータは、Cisco Meeting Management のポータルの会議のモニタリングと管理、システムのステータスチェック機能にのみアクセスすることができます。

展開の概要

標準的な展開では、複数の Unified CM ノードがコール制御に使用されます。Cisco Meeting Server は SIP トランクを使って Unified CM に接続し、会議リソースを管理したり、コールをブリッジしたりします。(C: 図 3-5) Cisco TMS および Cisco Meeting Management は、会議管理ファシリティとスケジューリングを提供します。同じインフラストラクチャが、非スケジュール済み会議とスケジュール済み会議の両方に使用されます。Cisco Expressway は、ローカルエンタープライズへの Business-to-Business (B2B) コールとモバイルおよびリモート アクセス (MRA) コールを可能にするためのファイアウォール トラバーサル機能を提供します。これらの要素は一緒に、ローカルエンタープライズに音声およびビデオ会議を提供します。

C: 図 3-5 標準的な展開



313344

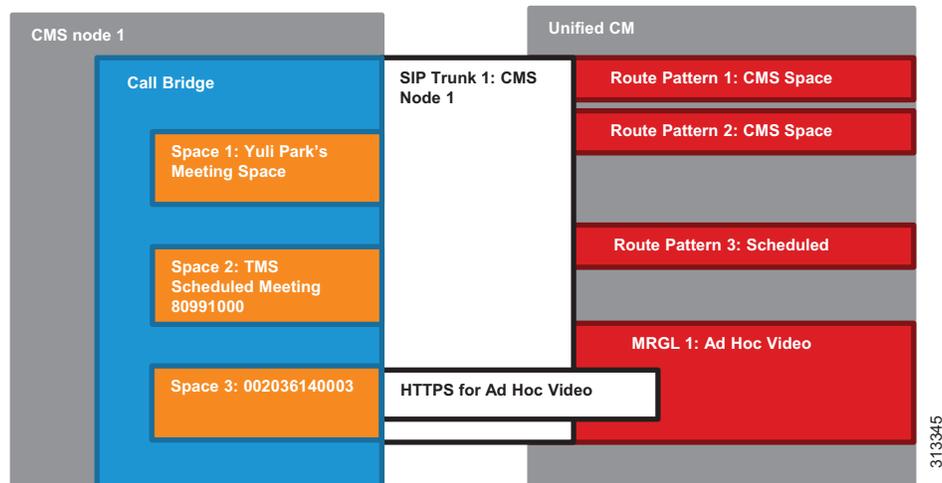
要件と推奨事項

- TelePresence コールを伝達する Unified CM に接続されたすべての SIP トランクで、早期オファーマッセージングを推奨します。
- Cisco Meeting Server ではすべての会議タイプ (インスタント、無期限、およびスケジュール済み) 用に 1 つの SIP トランクを使用します。
- Cisco Meeting Server で会議をホストするためのマルチパーティ ランセンスを設定します。

会議のコールフロー

Unified CM で、接続されたエンドポイント間の音声およびビデオ コールのデバイス登録およびルーティングを行います。無期限、インスタント、およびスケジュール済み会議のコールはすべて、単一の SIP トランクを介して Cisco Meeting Server 上の Call Bridge にルーティングされます。Call Bridge ごとに個別の SIP トランクが必要です。インスタント会議用に Cisco Meeting Server ノード宛てに XML-RPC 要求を送信する Unified CM ノードで、HTTPS 接続が設定されます (C : 図 3-6 を参照)。ユーザがデバイス上の会議ソフトキーを押して二者通話を三者通話にエスカレートすると、Unified CM が Cisco Meeting Server に API 要求を送信し、この HTTPS 接続を介して会議をホストするための一時スペースが作成されます。さまざまなコンポーネントによって作成されるスペース上で、インスタント、無期限、およびスケジュール済み会議がホストされます。スペースの詳細については、5. Cisco Meeting Server スペースを展開するのセクションを参照してください。

C : 図 3-6 Unified CM と Cisco Meeting Server SIP トランク



Unified CM によって管理されるインスタント コール フローは、スケジュール会議など、その他の方法で作成された会議への参加者を追加するために使用できません。その他のコール フローを使用して、インスタント会議への参加者を追加することはできません。インスタント コール エスカレーション方式は、その方法で作成されたインスタント会議でのみサポートされます。その他の方法で生成された会議をインスタント メカニズムで拡張することはできません。これにより、チェーン会議の可能性を回避できます。

インスタント会議

インスタント会議では、Unified CM と Cisco Meeting Server 上の Call Bridge の間で SIP トランクに関連付けられた HTTPS XML-RPC 接続が使用されます。ユーザが会議ソフトキーを押してインスタント会議を開始すると、Unified CM が HTTPS 接続を介して API 要求を発行し、Cisco Meeting Server 上で一時スペースが作成されます。その後、Unified CM は SIP トランクを介してすべての参加者をそのスペースにルーティングします。会議が終わると、Unified CM は別の API 要求を発行して、Cisco Meeting Server からそのスペースを削除します。

Cisco Meeting Server スペースを使用した常設会議

無期限会議は、Cisco Meeting Server スペースを使用して展開されます。スペースは、無期限タイプの会議を提供し、LDAP からのユーザインポートプロセスの一部として作成されます。ユーザは、いつでもスペース URI をダイヤルして会議を開始できます。管理者はフィールドマッピングを通してスペースの属性（名前、ユーザ名、URI など）を指定できます。これにより、これらのマッピングを使ってスペースを作成できるようになります。ユーザはその後、Cisco ミーティングアプリを使ってログインし、自分のスペースにメンバーを追加できます。Unified CM と、この会議タイプ用の Cisco Meeting Server 上の Call Bridge の間で SIP トランクを接続します。同じ SIP トランクが、他の会議タイプで会議参加者をスペースにルーティングするために使用されます。

スケジュール済み会議

このソリューションは Cisco Meeting Server 上の会議のスケジュールリングをサポートし、スケジュールリングは Cisco TMS を使用して実行されます。スケジュール済み会議では、Unified CM と、Cisco Meeting Server 上の Call Bridge の間に SIP トランクが必要です。ここでも、他の会議タイプの場合と同じ SIP トランクが使用され、Unified CM はスケジュール済み会議の参加者を SIP トランクの宛先にルーティングします。HTTPS 接続を介して Cisco Meeting Server 上で REST API 要求を発行できるようにするには、Cisco TMS に Cisco Meeting Server を追加します。スケジュール済み会議用の数値 ID 範囲を設定した後、Cisco TMS は API リンクを介して数値 ID ごとに Cisco Meeting Server 上に非アクティブなスペースを作成します。その後、Cisco TMS は、主催者が会議をスケジュールしたときにダイヤルイン番号をこの範囲からランダムに選択します。スケジュール済み会議を開始する時間になると、Cisco TMS は API を使用してスペースをアクティブにし、参加者がコールインを開始できるようになります。

サイドパーティー エンドポイント

他の機器プロバイダ製のエンドポイントは、標準的な SIP を使用して会議に参加できます。インスタント会議を開始できるのは、会議ボタンをサポートする Unified CM に登録されたエンドポイントだけです。SIP への H.323 コールをインターワーキングさせるために Cisco Expressway または Cisco VCS を使用できます。これにより、H.323 エンドポイントは会議に参加できるようになります。

ハイアベイラビリティ

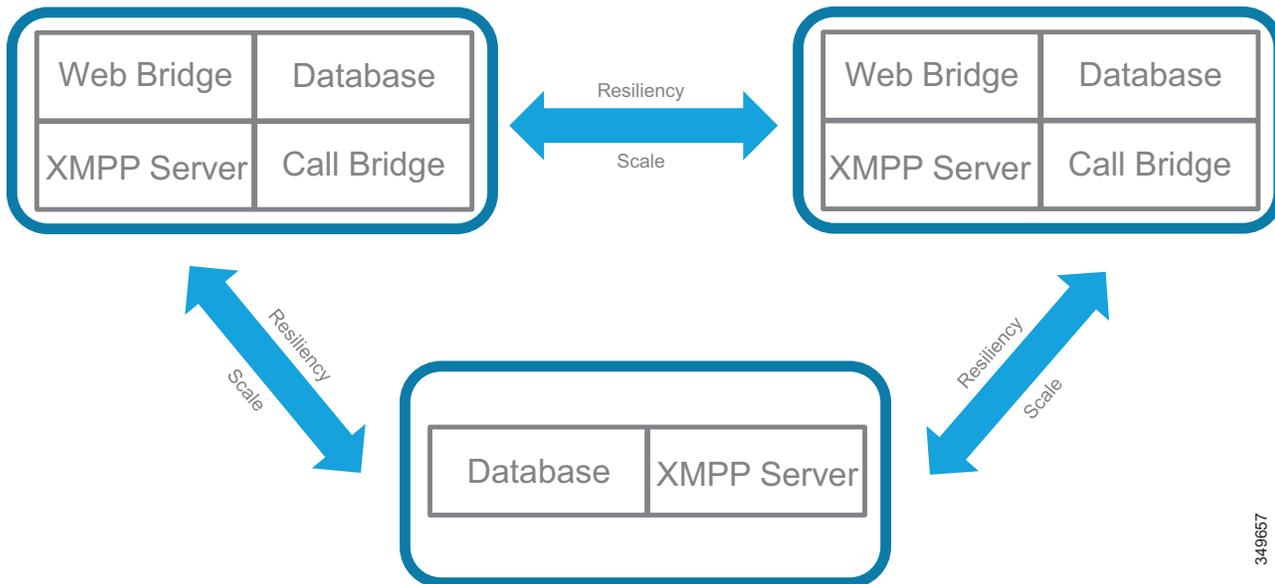
会議ソリューションについていくつかのレベルで、ハイアベイラビリティを考慮する必要があります。また、ハイアベイラビリティは、考慮するサービスに応じて異なる方法で実現されます。

スケジュール済み会議と非スケジュール済み会議の両方で、高可用性のために Cisco Unified CM、Cisco Meeting Server、および Cisco TMS が必要です。

Cisco Meeting Server の高適用性

追加のコンポーネントインスタンスを 1 つ以上のサーバに展開すると、Cisco Meeting Server の復元力が強化され、複数コンポーネントインスタンスで負荷を共有することができ、それらの 1 つで障害が発生してもバックアップインスタンスが負荷を処理します。加えて、XMPP サーバ、Call Bridge、およびデータベースをまとめてクラスタ化して単一のインスタンスとして動作させることができます。C : 図 3-7 を参照してください。

C : 図 3-7 高可用性を備えた Cisco Meeting Server クラスタの最小構成



349657

標準的な 1 つの Cisco Meeting Server クラスタは、Call Bridge サービスが有効になっている 2 つ以上（8 つ以下）のノードで構成されます。コールブリッジ間の最大ラウンドトリップ時間（RTT）は 300 ms です。Call Bridge クラスタ ピアは、分配リンクを介してフルメッシュ内で相互に接続されます。このリンクは、コールブリッジ間でコール信号と制御ステータスメッセージを渡すために使用される HTTPS 接続です。コールは、クラスタ内の任意のコールブリッジに送信することができます。1 つのコールブリッジがダウンした場合、統一された CM は残りの Call Bridge にコールをルーティングして会議に参加できるようにします。ライブ会議中に 1 つの Call Bridge で障害が発生した場合、それらのコールがドロップされ、参加者は同じ番号をダイヤルして新しい Call Bridge 上の会議に参加する必要があります。Unified CM ルートグループとルートリスト構造を使用すると、SIP トランクを介してコールを Cisco Meeting Server に分配できます。

1 つのクラスタとして構成された複数の Call Bridge を、1 つ以上の Call Bridge グループに分けることができます。グループ内の Call Bridge では、Cisco Meeting Server がそれらのブリッジ間でコールをインテリジェントに負荷分散して、可能な場合には同じ会議のすべてのコールを同じ Call Bridge に送信することができます。コールが Call Bridge に送信されると、Cisco Meeting Server は Call Bridge 内の現在の負荷に基づいてコールの拒否または受け入れを決定します。現在の負荷がプリセットしきい値を下回っている場合は、コールが受け入れられます。そうでない場合はコールが拒否され、Unified CM はダイヤルプラン設定を使用してそのコールを Call Bridge グループ内の別 Call Bridge に再ルーティングします。コールを受け入れる Call Bridge が Unified CM で見つからない場合は、コール全体が拒否されます。Cisco Meeting Server がコールを受け入れた後、コールをその Cisco Meeting Server の Call Bridge 上でホストすることも、会議の内部順序付きリストに従って優先順位が最も高い別の Call Bridge に移動することもできます。コールを移動した場合は、Call Bridge が有効になっているターゲット Cisco Meeting Server が Replaces を伴う INVITE を Unified CM に送ってコールを引き継ぎます。デフォルトで、Call Bridge グループ内の Call Bridge は、負荷が 80% になった時点で新しい参加者のコールをすべて拒否し、新しい分配コールだけが許可されます。コールブリッジ間のネットワーク要件としては、グループ内部のコールブリッジ間の RTT を 100 ms 以下に、同じクラスタ内の 2 つのコールブリッジ間の RTT を 300 ms 以下にする必要があります。



注

Call Bridge グループとロード バランシングが使用されない場合は、コールが拒否されませんが、負荷制限に到達したときにすべてのコールの品質が低下します。この現象が頻繁に起きる場合は、追加のハードウェアを配置することをお勧めします。

データベース クラスタは、1 つのマスターと複数のスレーブで構成されます。最大データベース数は 5 で、ノード間の最大 RTT は 200 ms です。データベース マスターは読み取り操作と書き込み操作の両方を実行できますが、スレーブは読み取り操作だけを実行できます。**Call Bridge** は常にデータベース マスターに接続して読み取りと書き込みを行い、マスターでのすべての変更内容がスレーブに複製されます。ローカル データベースを備えた **Call Bridge** は自動的にローカル データベース クラスタのマスターに接続しますが、ローカル データベースを備えていない **Call Bridge** は手動でデータベース クラスタに接続される必要があります。マスターで障害が発生すると、スレーブの 1 つが新しいマスターになり、他のスレーブがこの新しいマスターに対して再登録します。障害が修復されると、古いマスターがスレーブになり、新しいマスターに対して登録します。ネットワーク分割が発生した場合は、クラスタ メンバーの過半数を認識できるデータベース ノードのみが、マスターへの昇格対象と見なされます。同様に、クラスタ メンバーの過半数を認識できない既存のマスターはスレーブに降格されます。これにより、複数のマスターが作成されないことが保証されます。ここで、データベース クラスタが偶数 (2 つまたは 4 つ) のノードで構成され、等しいノード数の 2 つのセグメントにネットワークが分割された場合、一方の側のマスターが過半数の (つまり半数を超える) クラスタ メンバーを認識できないため、スレーブに降格されます。この場合、クラスタ内にマスターが存在しなくなり、**Call Bridge** は引き続きコールを引き受けますが、データベースの書き込み操作が不可能になります。このような理由で、マスターが常に選択されるようにするには、データベース クラスタのノード数を奇数にすることをお勧めします。その結果、クラスタ内のデータベース ノードの最小数は 3 になります。

XMPP の復元力により、特定の XMPP サーバに到達できないクライアント向けのフェールオーバー保護が提供されます。3 つ以上の奇数の XMPP サーバ ノードを使用して XMPP サーバ クラスタを設定する必要があります。これは、Cisco Meeting Server が XMPP サーバ マスターを選択するために過半数のクラスタ ノードが使用可能であるというマスター選択アルゴリズム要件があるためです。クラスタで XMPP サーバ マスターが使用可能でない場合、Cisco ミーティング アプリ ユーザはログインできません。各 XMPP サーバは、リンクが確立されている他のサーバの場所を認識しています。サーバはキープアライブ メッセージを使用して互いをモニタし、マスターを選出します。XMPP メッセージは任意のサーバに送られる可能性があり、マスター XMPP サーバに転送されます。マスターで障害が発生した場合は、新しいマスターが選択され、他の XMPP サーバは新しいマスターにメッセージを転送します。**Call Bridge** は DNS SRV レコード (`_xmpp-component`) を使用して、SRV レコードで設定された優先順位と重要度に基づいて利用可能な XMPP サーバと接続します。**Call Bridge** は、一度に 1 つの XMPP サーバに接続します。ネットワークの問題によって **Call Bridge** と XMPP サーバとの接続が失われた場合、**Call Bridge** は別の XMPP サーバに再接続しようとします。すべての **Call Bridge** をそれぞれの XMPP サーバ内で設定する必要があります。

C: 図 3-7 は、高可用性を備えた Cisco Meeting Server クラスタの最小設定を示しています。この構成では、データベースおよび XMPP サーバの 3 つのインスタンスをホストするために、最低 3 台のサーバが必要です。別個のサーバで各コンポーネント サービス (**Web Bridge** と **Call Bridge**) の少なくとも 2 つのインスタンスを有効にし、**Call Bridge** を 1 つのグループに配置します。各サーバ内のすべてのサービスを有効にする必要はありません。必要なものを有効にします。2 つの **Call Bridge** で処理できる以上のキャパシティが展開に必要な場合は、追加の **Call Bridge** を 3 番目のサーバでセットアップすることができます (**Call Bridge** 専用の 4 番目のサーバを調達する必要はありません)。**C: 表 3-3** は、単一の Unified CM クラスタ用のさまざまな数の **Call Bridge** に必要な Cisco Meeting Server クラスタ最小構成を示しています。

C : 表 3-3 単一の **Unified CM** クラスタ用のさまざまな数の **Call Bridge** に必要な **Cisco Meeting Server** クラスタ最小構成

Call Bridge グループ	コールブリッジの数	Cisco Meeting Server クラスタ構成
A	2	ノード A1 : Web Bridge、Call Bridge、データベース、XMPP ノード A2 : Web Bridge、Call Bridge、データベース、XMPP ノード A3 : XMPP、データベース
	3	ノード A1 : Web Bridge、Call Bridge、データベース、XMPP ノード A2 : Web Bridge、Call Bridge、データベース、XMPP ノード A3 : Call Bridge、データベース、XMPP
	4	ノード A1 : Web Bridge、Call Bridge、データベース、XMPP ノード A2 : Web Bridge、Call Bridge、データベース、XMPP ノード A3 : Call Bridge、データベース、XMPP ノード A4 : Call Bridge
	5	ノード A1 : Web Bridge、Call Bridge、データベース、XMPP ノード A2 : Web Bridge、Call Bridge、データベース、XMPP ノード A3 : Call Bridge、データベース、XMPP ノード A4 : Call Bridge ノード A5 : Call Bridge

TMS ハイ アベイラビリティ

大規模な Cisco TMS 展開の高可用性には、2つの TMS フロントエンドサーバ、TMSXE を実行する 2つのサーバ、ネットワーク ロード バランサ、および外部 Microsoft SQL データベースが含まれます (C : 図 3-2 を参照)。TMS 復元性では、2つのサーバ (1つのアクティブ ノードと 1つのパッシブ ノード) だけがサポートされており、またこのモデルでは、TMS 導入環境のキャパシティを増減することはできません。ネットワーク ロード バランサ (NLB) は、TMS サーバの前面に展開されます。TMS への着信トラフィックは、NLB を通過してアクティブ ノードに転送されます。TMS からの送信トラフィックは、NLB を通過せず直接、宛先に送信されます。NLB は既存のアクティブ ノードで障害を検出すると、ユーザによる介入なしで、自動的に新しいアクティブ ノードに切り替えます。

Cisco Meeting Management のハイ アベイラビリティ

Cisco Meeting Management には、復元力のためのクラスタ機能は組み込まれていません。高可用性のために、お客様は同一の設定で、2つの独立した Cisco Meeting Management インスタンスを設定できます。この場合、両方のインスタンスを同じ Cisco Meeting Servers と Cisco TMS に接続する必要があります。次に、ネットワークロードバランサーを Cisco Meeting Management インスタンスの前に配置すると、ユーザはロードバランサーを介して Cisco Meeting Management ポータルに接続することができます。Cisco Meeting Management サーバのロードバランサーの設定と可用性により、どの Cisco Meeting Management サーバにユーザが接続するかが判断されます。

会議のセキュリティー

プリファードアーキテクチャは、メディアとシグナリングの暗号化を完全にサポートします。ただし、このドキュメントで紹介するソリューションでは、簡略化のために、すべての会議用に Cisco Meeting Server と Unified CM の間に非セキュア SIP トランクを実装します。例外として、Unified CM と Cisco Meeting Server の間の API 通信を暗号化するというソリューション要件があるので、この場合は HTTPS を使用する必要があります。

Cisco Meeting Server は外部コンポーネントとの通信および内部コンポーネント間の通信にセキュア接続を使用するため、証明書が必要です。コンポーネント間の接続を保護するには、認証局 (CA) 署名付き証明書を使用します。詳細については、[セキュリティー](#)の章を参照してください。

PIN やパスワードを使用して会議へのアクセスを制限するため、別レベルのセキュリティーを追加できます。接続が許可される前にすべての参加者に PIN の入力を求めるように、すべてのスケジュール済み会議または無期限会議で PIN を設定できます。

会議ソリューションのスケールング

会議ソリューションを拡張する主な方法は、標準的な Cisco Meeting Server クラスタに (最大 8 つまで) Call Bridge を追加することです。

この展開では、Unified CM 内の SIP トランクを使用したダイヤルプラン、ルートグループ、およびルートリスト設定に基づいて、クラスタ内の任意の Call Bridge にコールをルーティングできます。同じ会議に対する複数コールが別々の Call Bridge にルーティングされる場合は、最後の 4 人のアクティブスピーカー (話者) の音声とビデオが Call Bridge 間で交換され、1 つのブリッジ上の参加者が別のブリッジ上のアクティブスピーカーを認識できます。



注

Cisco Meeting Server は、8 つを超える Call Bridge を使用したクラスタリングをサポートしますが、その展開にはシスコの事前承認が必要です。詳細については、地域のシスコアカウントチームにお問い合わせください。

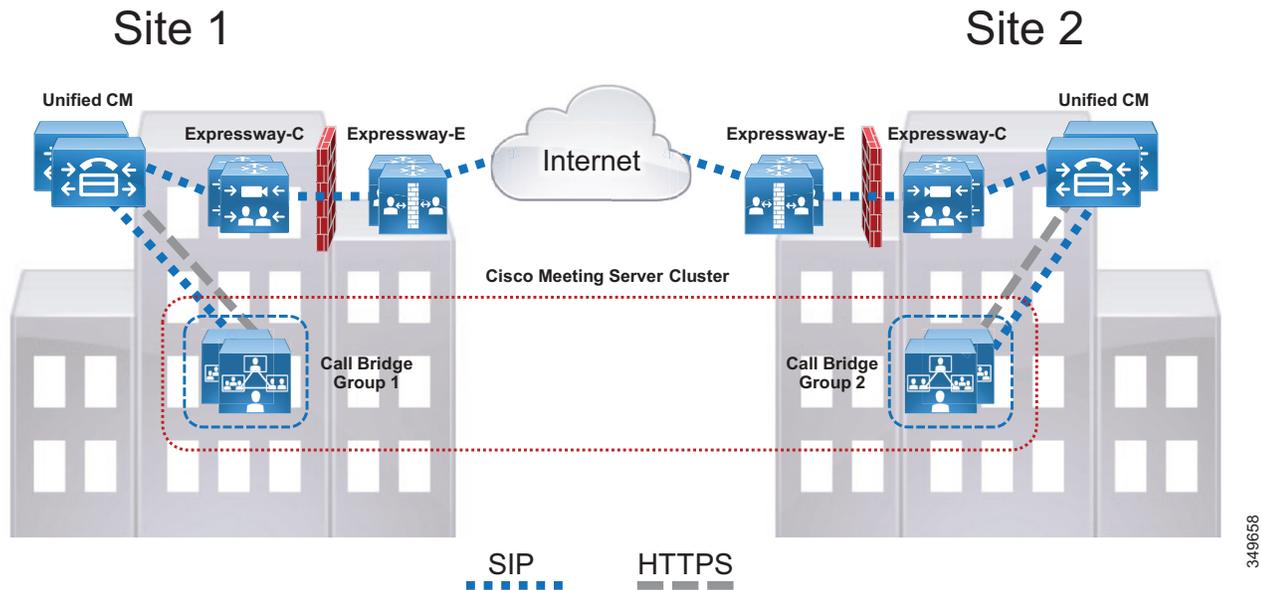
Call Bridge ごとに 450 人の参加者をサポートできます。そのため、会議ごとの参加者の最大数は単一のサーバで 450 人、1 つのクラスタ内の複数サーバでは最大 2,600 人の参加者をサポートできます。

複数の Unified CM クラスタに関する考慮事項

複数の Unified CM クラスタを含む大規模展開では、複数の Call Bridge グループを使って設定された 1 つの Cisco Meeting Server クラスタを使用し、Unified CM クラスタごとに 1 つのグループを割り当てます。

たとえば、展開に 3 つの Unified CM クラスタがある場合は、各 Unified CM クラスタに 1 つずつ、合計 3 つの Call Bridge グループを使用して 1 つの Cisco Meeting Server クラスタを展開する必要があります。各 Unified CM クラスタにおいて、ローカル Call Bridge グループ内の Call Bridge ごとに 1 つの SIP トランクが必要です。Unified CM クラスタへのすべての着信会議コールが、ローカル Call Bridge グループによって処理されます。Call Bridge には、フルメッシュ内のグループ内部および外部のピアに接続された分配リンクが必要です。同じ会議では、ユーザが Unified CM クラスタからダイヤルインしてローカル Call Bridge グループに到達できます。別々のグループ内の Call Bridge は、参加者がブリッジを超えて互いに認識できるように、最後の 4 人のアクティブスピーカーの音声とビデオをピアと交換します。(C : [図 3-8](#))。

C : 図 3-8 複数の Unified CM クラスタを使用した Cisco Meeting Server の展開



最初の Unified CM クラスタの設計については、Cisco Meeting Server の高適用性に関するセクションと C : 表 3-3 を参照してください。

2 番目の Unified CM クラスタでは、Cisco Meeting Server クラスタを拡張して 2 つの新しいサーバを追加します。それぞれのサーバで Web Bridge と Call Bridge を有効にします。この Unified CM クラスタでは、余分なデータベースや XMPP サービスは必要ありません。Call Bridge を既存のデータベース クラスタに接続し、すべての新しい Call Bridge を XMPP クラスタに追加します。この 2 番目の Unified CM クラスタで使用される新しい Call Bridge グループに Call Bridge を配置し、Web Bridge をこの Call Bridge グループに関連付けます。追加のキャパシティが必要な場合は、Call Bridge をホストする 1 つのサーバを追加して、その Call Bridge をこの 2 番目の Unified CM クラスタの Call Bridge グループに配置します。C : 表 3-4 は、必要な新しい Call Bridge の数に基づいて、2 番目の Unified CM クラスタに必要な追加の Cisco Meeting Server クラスタ構成を示しています。

C : 表 3-4 2 番目の Unified CM クラスタ用の追加の Cisco Meeting Server ノード構成

Call Bridge グループ	追加のコールブリッジの数	追加の Cisco Meeting Server ノード構成
B	2	ノード B1 : Web Bridge、Call Bridge ノード B2 : Web Bridge、Call Bridge
	3	ノード B1 : Web Bridge、Call Bridge ノード B2 : Web Bridge、Call Bridge ノード B3 : Call Bridge
	4	ノード B1 : Web Bridge、Call Bridge ノード B2 : Web Bridge、Call Bridge ノード B3 : Call Bridge ノード B4 : Call Bridge

3 番目の Unified CM クラスタでは、Cisco Meeting Server クラスタを拡張して 2 つのサーバを追加します。それぞれのサーバで Web Bridge と Call Bridge を有効にします。Call Bridge を既存のデータベース クラスタに接続し、すべての新しい Call Bridge を XMPP クラスタに追加します。この 3 番目の Unified CM クラスタで使用される新しい Call Bridge グループに Call Bridge を配置し、Web Bridge をこの Call Bridge グループに関連付けます。追加のキャパシティが必要な場合は、Call Bridge をホストする 1 つのサーバを追加して、その Call Bridge をこの 3 番目の Unified CM クラスタの Call Bridge グループに配置します。C : 表 3-5 は、必要な新しい Call Bridge の数に基づいて、3 番目の Unified CM クラスタに必要な追加の Cisco Meeting Server ノード構成を示しています。

C : 表 3-5 3 番目の Unified CM クラスタ用の追加の Cisco Meeting Server ノード構成

Call Bridge グループ	追加のコールブリッジの数	追加の Cisco Meeting Server ノード構成
C	2	ノード C1 : Web Bridge、Call Bridge ノード C2 : Web Bridge、Call Bridge
	3	ノード C1 : Web Bridge、Call Bridge ノード C2 : Web Bridge、Call Bridge ノード C3 : Call Bridge
	4	ノード C1 : Web Bridge、Call Bridge ノード C2 : Web Bridge、Call Bridge ノード C3 : Call Bridge ノード C4 : Call Bridge

3 つの Unified CM クラスタと 3 つの別々の Call Bridge グループを使用すれば、最初の Call Bridge グループに対してローカルな 3 つの XMPP およびデータベース クラスタ ノードを Call Bridge グループ間で分散できるため、Call Bridge グループごとに 1 つのローカル XMPP およびデータベース クラスタ ノードが割り当てられます。最初の Call Bridge グループに対してローカルな XMPP およびデータベース クラスタ ノードのうち 2 つをそれぞれ 2 番目と 3 番目の Call Bridge グループに移行することにより、すべての Call Bridge グループで XMPP および

データベース サービスの冗長性が確保されます。C : 表 3-6 は、この新しい Cisco Meeting Server クラスタ設定を示しています。

C : 表 3-6 2 番目と 3 番目の Call Bridge グループに XMPP およびデータベース サービスを移行する

Call Bridge グループ	Cisco Meeting Server クラスタ構成
A (Unified CM クラスタ 1)	ノード A1 : Web Bridge、Call Bridge、データベース、XMPP ノード A2 : Web Bridge、Call Bridge
B (Unified CM クラスタ 2)	ノード B1 : Web Bridge、Call Bridge、データベース、XMPP ノード B2 : Web Bridge、Call Bridge
C (Unified CM クラスタ 3)	ノード C1 : Web Bridge、Call Bridge、データベース、XMPP ノード C2 : Web Bridge、Call Bridge

展開に 4 番目の Unified CM クラスタが必要な場合は、Cisco Unified CM Session Management Edition 設計に移行することをお勧めします。ただし、このドキュメントではこれについて説明しません。

以降のガイドラインは、複数の Unified CM クラスタ用の別々のリージョンに Cisco Meeting Server クラスタを拡張する場合に当てはまります。

- 1 つの Cisco Meeting Server クラスタを 1 つ以上の Unified CM クラスタの展開に使用する必要があります。
- 標準的な Cisco Meeting Server クラスタに、最大 8 つの Call Bridge を展開することができます。8 つを超える Call Bridge をクラスタに展開する場合は、事前にシスコ アカウント チームの承認を得てください。
- Cisco Meeting Server クラスタに、最大 5 つのデータベースと奇数のノードを展開します。
- Cisco Meeting Server クラスタに、奇数の XMPP サービス ノードを展開します。
- ラウンドトリップ時間 (RTT) ネットワーク要件 :
 - Cisco Meeting Server クラスタ内の Call Bridge 間で最大 300 ms、データベース間で最大 200 ms
 - グループ内部の Call Bridge 間で最大 100 ms

会議の導入プロセス

会議ソリューションを導入するには、以下の主要なタスクをリストの順に実行します。

1. 会議の導入を計画する
2. Cisco Meeting Server を展開する
3. 会議用の Unified CM を有効にする
4. Cisco TelePresence Management Suite を展開する
5. Cisco Meeting Server スペースを展開する
6. Cisco Meeting Management の展開

1. 会議の導入を計画する

会議ソリューションを導入する前に、以下の項目について計画します。

要件

- 複数の DNS SRV レコードと A レコードが必要な Cisco Meeting Server の DNS を設定します。たとえば、Cisco ミーティング アプリは `_xmpp-client` SRV レコードを使用してユーザー認証用の XMPP サービスを検索します。
- Cisco Meeting Server では、導入を完了するために API を使用する必要があります。更新用の REST API コマンドを発行するために使用できるツール（Postman（<https://www.getpostman.com/>）など）を入手します。

ライセンス

さまざまな製品にライセンスをインストールする必要があります。

- Cisco TMS では、展開に十分なデバイス ライセンスをインストールする必要があります。
- Cisco Meeting Server では、Call Bridge を実行する各ノードに十分なマルチパーティ ライセンスをインストールする必要があります。

マルチパーティは、Cisco Meeting Server の展開に推奨されているユーザーベースのライセンスモデルです。Call Bridge サービスが有効になっているすべてのノードにこれを適用する必要があります。Personal と Shared の2つのバリエーションがあります。Personal Multiparty Plus (PMP+) は特定のネームドホスト用であり、Shared Multiparty Plus (SMP+) は会議室システム用またはユーザー間での共有用です。各ライセンスでは、ユーザーは、参加者数無制限、ビデオの最大解像度 1080p の会議をホストできます。C: 表 3-7 で、Personal Multiparty および Shared Multiparty の各ライセンスに含まれる機能を要約します。

C: 表 3-7 Cisco Personal および Shared Multiparty Plus ライセンスの機能

機能	Personal Multiparty Plus	Shared Multiparty Plus
ネームドホストとの関連付け	はい	いいえ (No)
アベイラビリティ	Cisco UWL Meetings に付属	個別に購入するか、またはルームシステムと共に割引価格で購入

C : 表 3-7 Cisco Personal および Shared Multiparty Plus ライセンスの機能 (続き)

機能	Personal Multiparty Plus	Shared Multiparty Plus
最小発注数	25	1
会議の最大参加者数	無制限 (利用可能なハードウェア キャパシティの制限内)	
最大解像度	ビデオ用の 1080p60 (フル HD) とコンテンツ用の 1080p30 シングル スクリーンまたはマルチ スクリーン エンドポイント	
Business-to-Business (B2B) または Business-to-Customer (B2C) 用のリッチ メディア セッション	同梱	同梱
Cisco TMS、TMSXE、および Skype for Business/Lync 相互運用 ライセンス	同梱	新規顧客は Starter Pack を購入 ¹
インスタント会議、無期限会議、およびスケジュール済み会議のサポート	はい	はい

1. TMS と関連製品のライセンスだけが必要な場合は、TMS Starter Pack をご購入いただけます。

マルチパーティ ライセンスは、プリファードアーキテクチャで使用されるライセンス モデルです。マルチパーティ ライセンスの詳細については、次の Web サイトで入手可能な『Cisco Multiparty Licensing At-a-Glance』を参照してください。

<https://www.cisco.com/c/dam/en/us/solutions/collateral/collaboration/pervasive-conferencing/at-a-glance-c45-729835.pdf>

Cisco TelePresence Management Suite

インストールと設定のプロセスを開始する前に、組織固有の構造と設定に合わせて各種アイテムを決定する必要があります。設定プロセス中にいくつかの設定値を使用する必要があるため、インストールプロセスの開始前にそれらの情報を収集してください。

Microsoft SQL

Cisco TMS は、会議、ユーザ、システムに関するすべてのデータを外部 Microsoft SQL データベースを使用して保存します。インストールプロセスでは、TMS と関連ソフトウェア拡張機能によって特定のデータベースがいくつか作成されます。TMS アプリケーションでは、tmsng データベースとの通信がアクティブでない場合には、ユーザは Web ページにログインできません。このように SQL データベースとの継続的な通信に依存しているため、SQL データベースでは、Microsoft によるデータベースの復元性を実現する手法も使用する必要があります。データベースのサイズは、導入の規模とスケジューリング イベントの数に応じて異なりますが、一般的な指針として、ほとんどの組織では初期ストレージとして 1 GB あれば十分です。

C : 表 3-8 に、Cisco TMS と TMSXE をサポートするために必要な Microsoft SQL 2012 の仕様を示します。

C:表 3-8 Cisco TMS と TMSXE のサポートに必要な Microsoft SQL 2012 の仕様

要件	パラメータ
TMS が使用するアカウントの SQL ユーザアカウント権限	dbcreator ロールと security admin ロール
認証	SQL Server および Windows 認証 (混合モード)
デフォルト言語	英語
タイムゾーン	TMS サーバのタイムゾーンに一致している必要があります
作成されるデータベース	tmsng (CiscoTMS)
復元性モデル	Windows Server フェールオーバー クラスタ (WSFC) による AlwaysOn フェールオーバー クラスタ インスタンス



注 その他の SQL 復元性モードが TMS でサポートされていますが、**AlwaysOn フェールオーバー クラスタ**以外の方法では、SQL の停止中に TMS 管理者が手動で調整を行う必要があります。

Active Directory

Cisco TMS は、Microsoft Active Directory のさまざまな側面と統合するので、サーバを組織のドメインに追加する必要があります。すべての TMS ユーザは Active Directory からインポートされ、Active Directory に対して認証されます。

設定プロセスでは、TMS がユーザをインポートできるようにするため、**AD サービス アカウントのユーザ名とパスワード**を入力する必要があります。これは読み取り専用アカウントであり、TMS が Active Directory の情報を変更することはありません。このアカウントには、AD 構造の最上位レベルへのアクセス権限が必要です。このアクセス権限により、後続のすべてのエンドユーザがその機能にアクセスできるようになります。複数ドメインを使用する組織では、TMS ユーザアカウントに最上位ドメインを関連付ける必要があります。エンドユーザが Exchange リソースを予約できるようにするため、TMSXE アプリケーションには追加のサービスアカウントが必要です。これも読み取り専用サービスアカウントである必要があります。また、実際のイベント予約にはエンドユーザのクレデンシャルが使用されます。TMSXE ユーザアカウントでは、TMSXE アプリケーションだけが Exchange Web Service を介して Exchange Server で認証および Exchange Server と通信できます。

また、AD で、TMS のスケジュール機能へのアクセス権限を持つエンドユーザと TMS 管理者の同期に使用する既存のグループを指定するか、または新規のグループを作成します。



注 TMS サーバのローカルマシンアカウントは、フロントエンドサーバ間で複製されないため、使用しないでください。また他のノードがアクティブになるとユーザクレデンシャルが使用できなくなります。

電子メールの統合

ユーザが会議をスケジュールすると、TMS は参加者のすべての接続情報を記載した自動メールをユーザに送信します。インストールプロセスで、この自動メールの送信元としてエンドユーザに対して表示される「from」アドレスを入力する必要があります。このため、collabconferencing@ent-pa.com のようなアドレス、または現在組織内で使用していない類似アドレスを選択します。

また、送信メールサーバの SMTP アドレスも入力する必要があります。

エンドポイントの命名規則

エンドポイントが Cisco TMS に追加される理由として、次の 2 つの理由があります。

- 会議リソースの割り当てのために Exchange リソースを関連付ける
- TMS がワンボタン機能の接続情報をエンドポイント ユーザ インターフェイスに提供できるようにする

TMS にエンドポイントが追加されると、Exchange でルーム名またはリソース名として同じ文字列が使用されます。これにより、エンドユーザに対して、コール履歴にシステム名が表示される時に統一がとられます。また、画面上のラベルのテキストが会議リソースから取り込まれます。

TMS Systems Navigator のフォルダ構造の使用法について系統立った計画を立てることで、管理者が簡素化されたインターフェイスを使用できるようになります。

組織のデフォルト会議パラメータ

これは組織別にカスタマイズ可能な設定であり、各自のネットワークに関する考慮事項、会議の流れ、企業風土に基づいて使用する必要があります。エンドユーザが Outlook 経由でスケジュールしたすべての会議に、デフォルトの会議設定が使用されます。デフォルトの会議のさまざまな設定については、次の場所にある『Cisco TelePresence Management Suite Administrator Guide』の最新版を参照してください。

<https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html>

Cisco Meeting Server スペースのプロビジョニング

組織で Cisco Meeting Server スペースをどのように利用すべきかを理解するには、エンドユーザたちが会議で想定するワークフローについて理解する必要があります。組織によっては、特にスタッフが別々の場所において共通の会議室に集合できないような場合に、特定の会議タイプにスケジュール済みリソースの代わりにスペースを活用することができます。

サーバのロケーション

冗長 TMS 導入環境のアクティブ ノードとパッシブ ノードの両方に対し、サーバオペレーティング システムで同一タイムゾーンを設定する必要があります。また、これは SQL サーバと同じタイムゾーンである必要もあります。冗長 TMS のサポートは、アクティブ ノードとパッシブ ノードの両方と SQL サーバが同じローカル ネットワーク上に存在する場合に限定されています。

2. Cisco Meeting Server を展開する

このセクションでは、Cisco Meeting Server を展開してスケジュール済み会議と非スケジュール済み会議用にそれらを準備するのに必要な主なタスクについて説明します。

概要

Cisco Meeting Server の展開タスク：

1. Cisco Meeting Server 機能ライセンス キーをインストールします。
2. エンタープライズ CA 署名付き証明書を生成します。
3. Web 管理、XMPP、Call Bridge、および Web Bridge サービスを設定します。
4. 冗長性のために追加のノードをセットアップし、XMPP、データベース、および Call Bridge のクラスタリングを設定します。
5. 分散会議用の Call Bridge クラスタ ピアにコールを送信するアウトバウンドダイヤルプランをセットアップします。
6. Call Bridge グループを 1 つ作成し、Unified CM クラスタ用にすべての Call Bridge をそのグループに追加します。
7. コール設定のパラメータを更新します。

展開の考慮事項

メディアトラフィックが Cisco Meeting Server と会議の各参加者との間を流れるので、Cisco Meeting Server の物理的な場所を考慮することが重要です。参加者に最高のエクスペリエンスを提供するには、Call Bridge を使用する Cisco Meeting Server の場所を集中させ、それらのブリッジを各リージョンの Unified CM クラスタ用の 1 つのグループに配置します。

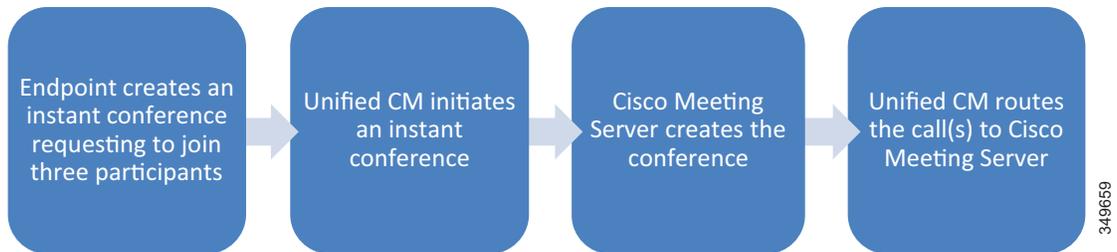
展開に Cisco Meeting アプリあるいは Web Bridge が含まれている場合は、XMPP サーバを有効にして、ユーザ認証用の XMPP ドメインを使ってそれを設定する必要があります。親ドメイン (ent-pa.com など) を XMPP ドメインとして使用することを避けてください。これは、そのドメインが Cisco Unified CM IM and Presence Service などの他のコンポーネントですでに使用されている可能性があり、その場合には全体の設計が複雑になるためです。Cisco Meeting Server 用の XMPP ドメインとしてサブドメイン (cms.ent-pa.com など) を使用することをお勧めします。

XMPP サーバ/データベース用の 3 ノードクラスタを展開します。これにより、ほとんどの展開シナリオで復元力と高可用性が提供されるはずですが。

各 Web Bridge に同じ名前 (join.ent-pa.com など) を使用して DNS A レコードを作成します。そうすれば、会議に参加するために使用する Web Bridge URL (たとえば <https://join.ent-pa.com>) を参加者が覚えやすくなります。

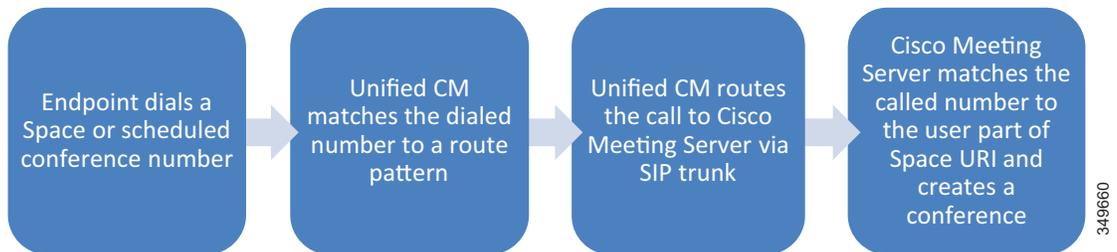
インスタント、無期限、およびスケジュール会議

C : 図 3-9 インスタント会議のコールフロー



349659

C : 図 3-10 無期限またはスケジュール会議のコールフロー



349660

Cisco Meeting Server の展開タスク

Cisco Meeting Server は、Call Bridge ライセンスなしでコールを受け取ることができません。Call Bridge、マルチパーティ ライセンス、その他の機能ライセンスが **cms.lic** という名前の単一のライセンス ファイルにバンドルされています。SFTP クライアント ソフトウェアを使用して、ライセンス ファイルをそれぞれの Cisco Meeting Server にアップロードします。ライセンス ファイルは Cisco Meeting Server の MAC アドレスに対応付けられます。このため、正しいファイルに対応するサーバにアップロードする必要があることに注意してください。

エンタープライズ CA 署名付き証明書の生成方法の詳細については、[セキュリティ](#)の章の [Cisco Meeting Server](#) のセクションを参照してください。これにより、2つの証明書が生成されます。1つは、任意のノード内の Web 管理、XMPP、Call Bridge、Web Bridge、およびデータベース クラスタ用に共有される証明書で、もう1つは、データベース クラスタへの接続用にローカル データベースを備えていない Call Bridge によって使用される証明書です。

これが Call Bridge ノードでない場合は、省略してください。

Web 管理では、メインボード管理プロセッサ (MMP) コマンドを使用してリスニング インターフェイスとポートを指定し、共有 CA 署名付き証明書をインストールして、サービスを有効にします。これにより、管理者は、指定されたリスニング インターフェイスおよびポートを使用して Web インターフェイスにアクセスすることができます。デフォルトでは、Web 管理と Web Bridge の両方がポート 443 を使用します。この両方がポート 443 を使用する場合は、別々のネットワーク インターフェイスを使用する必要があります。しかし、同じインターフェイスを使用する場合は、どちらかのサービスが別のデフォルト ポートを使用する必要があります。その場合、Web 管理のデフォルト ポートを、他の使用されているポート (ポート 445 など) に変更することをお勧めします。

Call Bridge では、MMP コマンドを使用してリスニング インターフェイスを指定し、共有 CA 署名付き証明書をインストールして、サービスを再起動します。

XMPP サーバでは、MMP コマンドを使用してリスニング インターフェイスと XMPP ドメイン (cms.ent-pa.com など) を指定し、共有 CA 署名付き証明書をインストールして、サービスを有効にします。最初の XMPP サーバでは、必要な数の Call Bridge を追加し、各 Call Bridge に一意の名前を割り当て、生成された名前と秘密文字列を書き留めます。後続の XMPP サーバでは、最初の XMPP サーバで生成された Call Bridge 名と秘密文字列を使用して、必要な数の Call Bridge を追加します。

これが **Call Bridge** ノードでない場合は、省略してください。

Web インターフェイス ([設定 (Configuration)] -> [全般 (General)]) に移動し、C : 表 3-9 の値を使用して XMPP サーバ設定を構成します。

C : 表 3-9 最初の Call Bridge 用の XMPP サーバ設定

フィールド名	値
一意の Call Bridge 名 (Unique Call Bridge name)	< 一意の Call Bridge 名 >
ドメイン (Domain)	cms.ent-pa.com
サーバアドレス (Server address)	空白のまま
共有秘密 (Shared secret)	<Call Bridge の秘密文字列>

Web Bridge では、MMP コマンドを使用してリスニング インターフェイスを指定し、共有 CA 署名付き証明書をインストールし、上記でインストールした Call Bridge 証明書に対する信頼を有効にして、サービスを有効にします。Web Bridge は、WebRTC クライアントからの接続を受け入れた後で Call Bridge に接続するので、Call Bridge からの証明書を信頼する必要があります。

クラスタ内のすべてのノードに対して上記の手順を繰り返します。

データベース クラスタをセットアップします。

各データベース ノードで MMP コマンドを使用して、データベースによって使用されるネットワーク インターフェイスを指定し、共有 CA 署名付き証明書をインストールします。1 つのノードをマスターとして選択し、MMP コマンドを実行してデータベースを初期化します。各データベース スレーブ ノードに移動し、MMP コマンドを実行してデータベースとクラスタを接続します。ローカル データベースを備えていない Call Bridge が配置されたすべてのノードで、2 番目の証明書をインストールし、MMP コマンドを実行してクラスタに接続します。次のコマンドに移る前に、コマンドの実行ステータスが「成功」になっていることを確認してください。これで、データベース クラスタのセットアップが完了しました。



警告

スレーブ データベース内のデータは、スレーブがクラスタに参加した後、マスターによって上書きされます。

Call Bridge クラスタをセットアップします。

各 Call Bridge ノードで、Web インターフェイス ([設定 (Configuration)] -> [クラスタ (Cluster)]) に移動して、Call Bridge の [ID (Call Bridge identity)] の下で一意の名前 (callbridge1 など) を設定します。その後、いずれかの Call Bridge ノードでクラスタの設定 ([設定 (Configuration)] -> [クラスタ (Cluster)]) に戻り、C : 表 3-10 の例を参考にして [クラスタ化された Call Bridges (Clustered Call Bridges)] にすべての Call Bridge に関する情報を入力し、その他のフィールドを空白またはデフォルトのままにします。

C : 表 3-10 クラスタ化された Call Bridge の設定例

一意の名前	アドレス	コメント
callbridge1	https://10.x.x.60:445	[アドレス (Address)] 列は、Web インターフェイスにアクセスするために使用される URL とポート番号です。
callbridge2	https://10.x.x.61:445	
callbridge3	https://10.x.x.62:445	

[クラスタ化された Call Bridge (Clustered Call Bridges)] の設定は、Web インターフェイスからすべての Call Bridge ノードに表示されます。これらは、分散会議用にピア間でコール信号とステータスメッセージを渡すために Call Bridge で使われる分配リンクです。

API を使用して、分散会議用のコールブリッジクラスタピアにコールを送信するためのアウトバウンドダイヤルプランルールをセットアップします。各コールブリッジには、コール制御ではなく直接ピアにコールをルーティングするように、各ピアに対して設定された発信ダイヤルプランルールを設定する必要があります。クラスタ内に 3 つの Call Bridge が存在する場合は、Call Bridge ごとに 2 つのアウトバウンドダイヤルプランルールを設定する必要があります。クラスタ内で設定されるアウトバウンドダイヤルプランルールは全部で 6 つになります。/callBridges ノードで GET メソッドを使用して、Cisco Meeting Server クラスタ内のすべての Call Bridge の ID を取得します。C : 表 3-10 の [クラスタ化された Call Bridge (Clustered Call Bridges)] の設定例を参考にして、C : 表 3-11 の各行をパラメータ設定として使用し、/outboundDialPlanRules ノードで POST メソッドを実行します。

C : 表 3-11 アウトバウンドダイヤルプランルールのパラメータの例

ドメイン	プライオリティ	スコープ	trunkType	callBridge
10.x.x.61	100	callBridge	sip	<callbridge1 ID>
10.x.x.62	100	callBridge	sip	<callbridge1 ID>
10.x.x.60	100	callBridge	sip	<callbridge2 ID>
10.x.x.62	100	callBridge	sip	<callbridge2 ID>
10.x.x.60	100	callBridge	sip	<callbridge3 ID>
10.x.x.61	100	callBridge	sip	<callbridge3 ID>

展開された Web Bridge ごとに、Call Bridge は Web Bridge にアクセスするための URL を認識する必要があります。C : 表 3-12 の各行の URL パラメータを使用して、/webBridges ノードで POST メソッドを実行します。

C : 表 3-12 Web Bridge の設定例

Web Bridge の IP アドレス	URL
10.x.x.60	https://10.x.x.60
10.x.x.61	https://10.x.x.61

XMPP サーバ クラスタをセットアップします。

1 つのノードをマスターとして選択し、MMP コマンドを実行してクラスタを有効化および初期化し、共有 CA 署名付き証明書を信頼するようにクラスタをセットアップします。残りの XMPP サーバで、MMP コマンドを実行してクラスタリングを有効にし、クラスタに参加させて、共有 CA 署名付き証明書を信頼するようにクラスタをセットアップします。次のコマンドに移る前に、各コマンドが正常に実行されたことを確認してください。

C : 表 3-13 に示すように、XMPP サーバ ノードごとに DNS SRV レコードを作成します。

C : 表 3-13 XMPP サーバ用の DNS SRV レコード

名前	解決先	ポート	説明
_xmpp-client._tcp.<XMPPDomain>	XMPP サーバの FQDN	5222	ログイン認証用の XMPP サーバを検索するために Cisco ミーティング アプリで使用される
_xmpp-component._tcp.<XMPPDomain>	XMPP サーバの FQDN	5223	使用可能な XMPP サーバを検索するために Call Bridge で使用される

各 Web Bridge で同じ名前 (join.ent pa.com など) を使用して、Web Bridge によって使用されるインターフェイスの IP アドレスに解決される DNS A レコードを作成します。

パラメータ **loadBalancingEnabled** を **true** に設定した API (POST/callBridgeGroups) を使用して、ロード バランシング オプションが有効化された Call Bridge グループを作成し、返された Call Bridge グループの GUID を書き留めます。各 Call Bridge で API (PUT/callBridges) を使用して、Call Bridge をグループに追加するために **callBridgeGroup** パラメータを <callBridgeGroup GUID> に設定します。API (PUT/system/configuration/cluster) を使用して、サーバプラットフォームの最大負荷に関する **loadLimit** パラメータ値を設定します。その際、次の場所にある『Load Balancing Calls Across Cisco Meeting Servers』に関するホワイトペーパーの最新版で指定されているプラットフォーム依存値を使用してください。

<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html>

各 Web Bridge で、API (PUT/webBridges) を使用して **callBridgeGroup** パラメータを <callBridgeGroup GUID> に設定することで、グループ内の Call Bridge のみが Web Bridge への接続を試みるように Web Bridge と Call Bridge グループを関連付けます。

この時点で、完全な Cisco Meeting Server クラスタが設定されるはずですが、いずれかの Web 管理ページを参照し、C : 表 3-14 の値を使用して、Web インターフェイス ([設定 (Configuration)]->[全般 (General)]) でコール設定パラメータを更新します。

C : 表 3-14 コール設定の構成例

フィールド名	値	コメント
SIP メディア暗号化	[許可 (allowed)]	RTP と SRTP の両方を許可する
SIP コール参加者ラベル	[有効 (enabled)]	表示名を表示する (レイアウトでサポートされている場合)
TIP コール	[有効 (enabled)]	TIP の使用を許可する

要約

上記のタスクが完了したら、Cisco Meeting Server を Unified CM に追加する準備が整います。

3. 会議用の Unified CM を有効にする

このセクションでは、Cisco Meeting Server クラスタを使用した会議用に Unified CM を有効にするために必要な主なタスクを説明します。

概要

インスタント会議用に Unified CM を有効にするための展開タスク：

1. 「**Standard SIP Profile for CMS**」という名前の新しい SIP プロファイルと、「**Security SIP Trunk Profile for CMS**」という名前の SIP トランク セキュリティプロファイルを作成します。
2. Cisco Meeting Server の Call Bridge ノードを指し示す SIP トランク (SIP_TRUNK_CMS1) を作成します。この手順を、Cisco Meeting Server クラスタ ノード内の各 Call Bridge に対して繰り返す必要があります。たとえば、クラスタ内に 3 つの Call Bridge が存在する場合は、設定された 3 つの SIP トランクが存在する必要があります。
3. 1 つの会議ブリッジを作成し、SIP トランク (タスク 2 で設定済み) をそれに追加します。各会議ブリッジに、いずれかの Call Bridge クラスタ ピアへの SIP トランクが含まれている必要があります。

API 特権を持つ Cisco Meeting Server 上で作成されたユーザ名とパスワードを使って各会議ブリッジを設定します。

この手順を、Cisco Meeting Server クラスタで有効になっている各 Call Bridge で繰り返す必要があります。たとえば、クラスタ内に 3 つの Call Bridge が存在する場合は、設定された 3 つの会議ブリッジが存在する必要があります。

4. **Video** という名前のメディア リソース グループ (MRG) を作成します。すべての会議ブリッジを MRG に追加します。クラスタ内に 3 つの Call Bridge が存在する場合は、MRG 内に 3 つの会議ブリッジが存在する必要があります。
5. **Video** という名前のメディア リソース グループ リスト (MRGL) を作成して、MRG (タスク 4 で設定済み) をそれに追加します。エンドポイントによるインスタント会議の使用を許可するには、MRGL をデバイス プールまたはデバイス自体に割り当てます。

無期限会議とスケジュール済み会議用に Unified CM を有効にするための展開タスク：

6. 無期限会議とスケジュール済み会議用のルート グループ (RG_SPACE_SCHED) を作成します。すべての SIP トランク (タスク 2 で設定済み) をルート グループに追加します。クラスタ内に 3 つの Call Bridge ノードが存在する場合は、ルート グループ内に、それぞれ Call Bridge ノードのいずれかを指し示す 3 つの SIP トランクが存在する必要があります。
7. ルート リスト (RL_SPACE_SCHED) を作成し、それにルート グループを追加します。
8. [4. Cisco TelePresence Management Suite を展開する](#) のセクションで設定するスケジュール済み会議の数字エイリアスと一致するルート パターン (8099[12]XXX) を作成します。スペースを設定する場合には、さらに追加のルート パターンが必要になります。それらについては、[5. Cisco Meeting Server スペースを展開する](#) のセクションで説明します。

展開の考慮事項

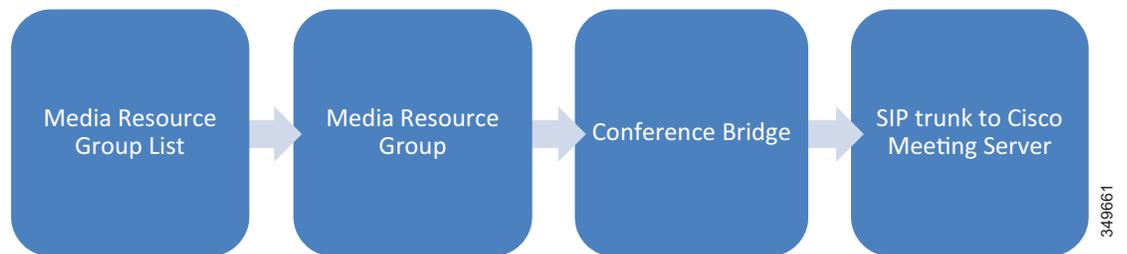
Unified CM は、会議を開始するために Cisco Meeting Server へのコールをどのようにルーティングするかを記述する最初の論理点です。Unified CM でのインスタント会議と無期限 / スケジュール済み会議の設定手順は異なります。これは、それぞれのタイプの会議に参加するためのメカニズムが異なるためです。



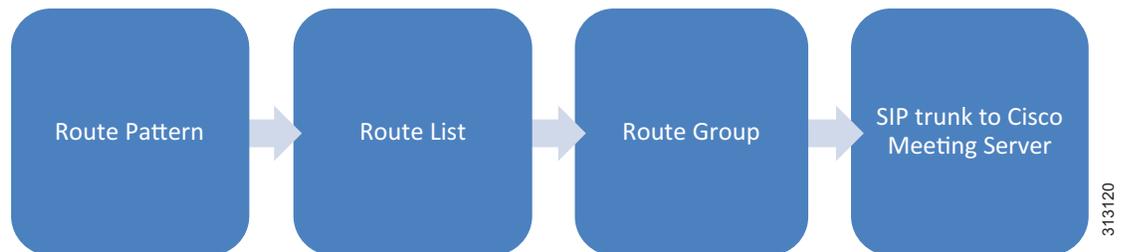
注 インスタント会議を開始するために使用するエンドポイントには、会議ボタンが必要になります。会議ボタンがないエンドポイントもインスタント会議に参加することはできますが、会議ボタンがあるエンドポイントに、会議に追加してもらう必要があります。

インスタントおよび無期限の会議

C : 図 3-11 インスタント会議用の Unified CM の内部設定フロー



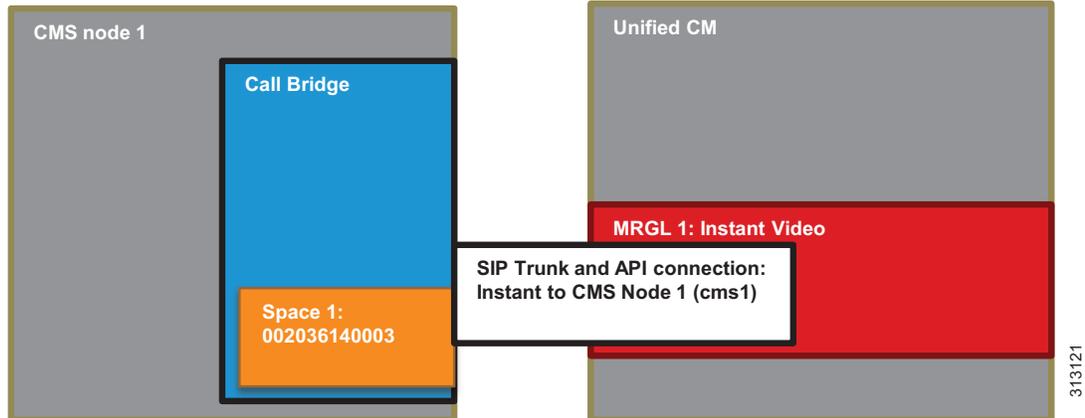
C : 図 3-12 無期限会議とスケジュール済み会議用の Unified CM の内部設定フロー



インスタント会議用に Unified CM を有効にするための展開タスク

Unified CM 内の SIP トランクは Cisco Meeting Server 内の Call Bridge を指し示す必要がありますが、API 接続は Web 管理インターフェイスとポートを指し示す必要があることを理解することが重要です。HTTPS を使用して API 接続を保護する必要があります。すべての会議タイプに対して同じ SIP トランクを使用することができます。Cisco Meeting Server クラスタ内の各 Call Bridge ノードには、SIP トランクと Unified CM 内の会議ブリッジからの API 接続で構成される一意のセットが必要です (C : 図 3-13)。

C : 図 3-13 Cisco Unified CM と Cisco Meeting Server のインスタント関係



Cisco Meeting Server への SIP トランクですべてのシナリオのコールをサポートするには、カスタマイズされた SIP プロファイルと SIP トランク セキュリティ プロファイルが必要です。SIP プロファイルを作成するには、**Standard SIP Profile for TelePresence Conferencing** をコピーして、そのコピーに「**Standard SIP Profile for CMS**」という名前を付け、C : 表 3-15 に示されているように設定を変更します。

C : 表 3-15 SIP プロファイルの設定

設定	値	コメント
[音声コールとビデオコールに対する早期オファーサポート (Early Offer support for voice and video calls)]	[ベストエフォート (MTP の挿入なし)]	これは、すべての Unified CM トランクに対して推奨される設定です。ベストエフォートの早期オファー トランクでは、早期オファーを作成するために MTP を使用しません。コールに使用するデバイスに応じて、早期オファーか遅延オファーのいずれかを使用して発信 SIP トランク コールを開始します。この設計では、発信コールは常に早期オファーを使用します。

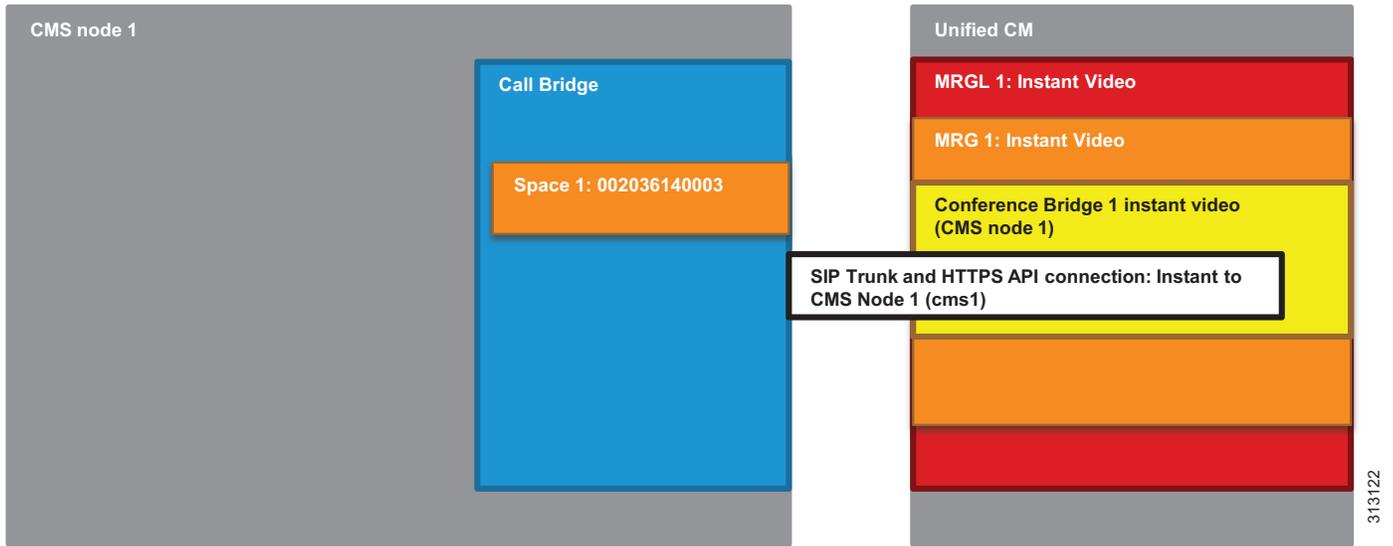
SIP トランク セキュリティ プロファイルを作成するには、**Non Secure SIP Trunk Profile** をコピーして、そのコピーに「**Security SIP Trunk Profile for CMS**」という名前を付け、C : 表 3-16 に示すように設定を変更します。

C : 表 3-16 SIP トランク セキュリティ プロファイルの設定

設定	値	コメント
[Replaces ヘッダーの許可 (Accept replaces header)]	オン	Call Bridge グループ内の該当する Cisco Meeting Server にコールを再ルーティングするための Replaces ヘッダーを伴う INVITE を Unified CM で受け入れるには、このオプションを有効にします。

SIP トランクは、Unified CM に SIP トラフィックをルーティングする場所を伝達します。インスタント会議の場合、SIP トランクは Unified CM に API 要求の宛先も伝達し、それらは会議ブリッジ設定 (C : 図 3-14) で使用されます。Cisco Meeting Server 内の Call Bridge に接続される SIP トランクを、セキュリティで保護するように設定できますが、このガイドでは、セキュリティで保護しない設定を想定しています。

C : 図 3-14 Cisco Unified CM のインスタント設定



会議ブリッジ設定によって、2つの重要な情報（Cisco Meeting Server と通信するための API クレデンシャルと、その通信用の宛先アドレス）が Unified CM に通知されます（C : 図 3-14）。ユーザ名とパスワードが、Cisco Meeting Server で設定された API ユーザのものと一致する必要があります。会議ブリッジで設定された SIP トランクは、HTTPS API トラフィックの送信先を Unified CM に示します。各 SIP トランクは、C : 表 3-17 に示す設定で設定します。加えて、各 Unified CM クラスタには、会議ブリッジで設定された一意の会議ブリッジプレフィックスが必要です。このプレフィックスは単一 Unified CM クラスタの操作には影響を与えませんが、マルチクラスタ Unified CM 展開では、このプレフィックスにより、2つの Unified CM クラスタが同じミーティング番号を同時に別々のインスタント会議に割り当てるのが防止されます。

C : 表 3-17 インスタント会議用の SIP トランク設定

設定	値	コメント
名前	SIP_TRUNK_CMS1	Call Bridge が有効になっている Cisco Meeting Server ノード 1 を指し示す SIP トランクの名前
[説明 (Description)]		わかりやすい説明
[デバイスプール (Device Pool)]	[Trunks_and_Apps]	中央トランクの共通デバイス プール
[メディアリソースグループリスト (Media Resource Group List)]	< なし >	デバイス プールで定義された MRGL を使用する
[AAR グループ (AAR Group)]	[デフォルト (Default)]	すべての場所で同じ
[発呼側名に UTF-8 を転送 (Transmit UTF-8 for Calling Party Name)]	オン	この設定によって、ASCII 呼び出し表示を、UTF-8 文字をサポートするデバイスに転送できます。
[PSTN アクセス (PSTN Access)]	オフ	
[すべてのアクティブな Unified CM ノードで実行 (Run on All Active Unified CM Nodes)]	オン	すべての SIP トランクで、この設定が推奨されています。この設定によって、SIP への発信コールは、Unified CM コール処理サブスクライバ間のクラスタ内制御シグナリングを必要としなくなります。

C : 表 3-17 インスタント会議用の SIP トランク設定 (続き)

設定	値	コメント
着信コール		
[コーリングサーチスペース (Calling Search Space)]	[TelePresenceConferencing]	コール制御の章で定義されているとおり
[AAR コーリングサーチスペース (AAR Calling Search Space)]	[PSTNReroute]	
[アウトバウンドコール (Outbound Calls)]		
[デバイスプールの着信側トランスフォーメーション CSS を使用 (Use Device Pool Called Party Transformation CSS)]	オン	
[デバイスプールの発呼側トランスフォーメーション CSS を使用 (Use Device Pool Calling Party Transformation CSS)]	オン	
[SIP 情報 (SIP Information)]		
接続先	us-cms1.ent-pa.com	Cisco Meeting Server ノード 1 の FQDN
[SIP トランクセキュリティプロファイル (SIP Trunk Security Profile)]	CMS のセキュリティ SIP トランク プロファイル	上記で作成した SIP トランク セキュリティプロファイルを使用します。
再ルーティング用コーリングサーチスペース (Rerouting Calling Search Space)	TelePresenceConferencing	上記で着信コールに関して設定したものと同一コーリングサーチスペースを使用します。
[SIP プロファイル (SIP Profile)]	CMS の標準 SIP プロファイル	上記で作成した SIP プロファイルを使用します。

すべての会議ブリッジを設定したら、それらをメディア リソース グループ (MRG) に追加できます。各メディア リソース グループでは、1 つの Call Bridge ノードが通信不能になった場合にコールを別のノードにルーティングできるように、Cisco Meeting Server ノード内の各 Call Bridge から 1 つの会議ブリッジを含める必要があります。

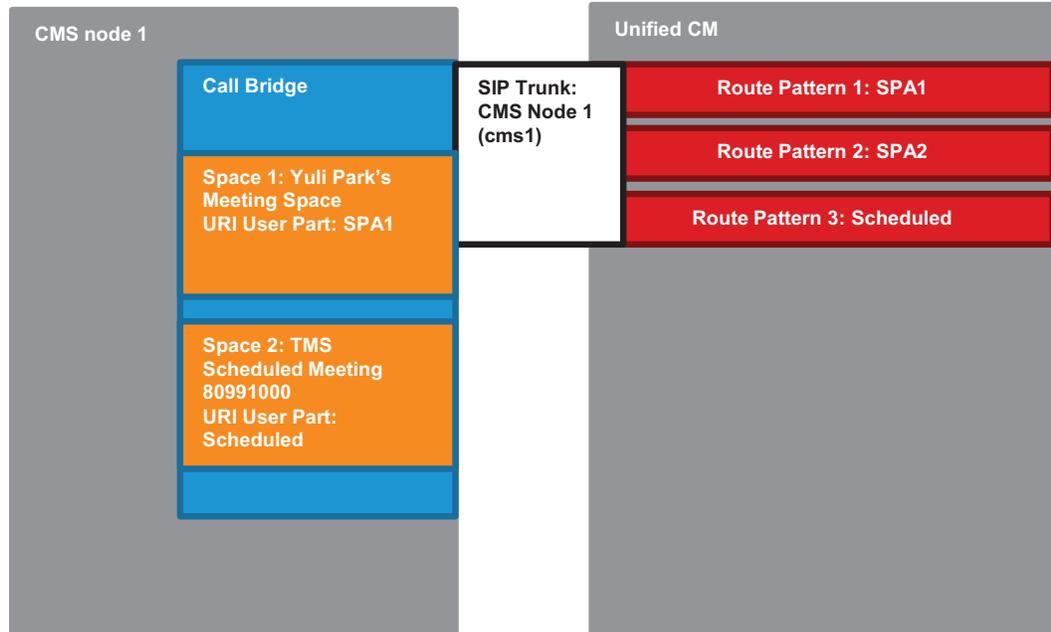
各メディア リソース グループは、独自のメディア リソース グループ リスト (MRGL) に追加できます。メディア リソース グループ リストは、Unified CM 内のデバイスまたはデバイス プールに割り当てることができます。また、会議ボタンを使用して、ポイントツーポイント コールから会議コールにそれらのデバイスをエスカレートするときに使用できます。

Cisco Meeting Server 内部では、ユーザがデバイスで会議ボタンを押してエスカレーションを開始したときに、インスタント会議によって使用されるスペースが HTTPS API 接続を介して動的に作成されます。このスペースは、会議の終了後に、API 接続を介して削除されます。

無期限会議とスケジュール済み会議用に Unified CM を有効にするための展開タスク

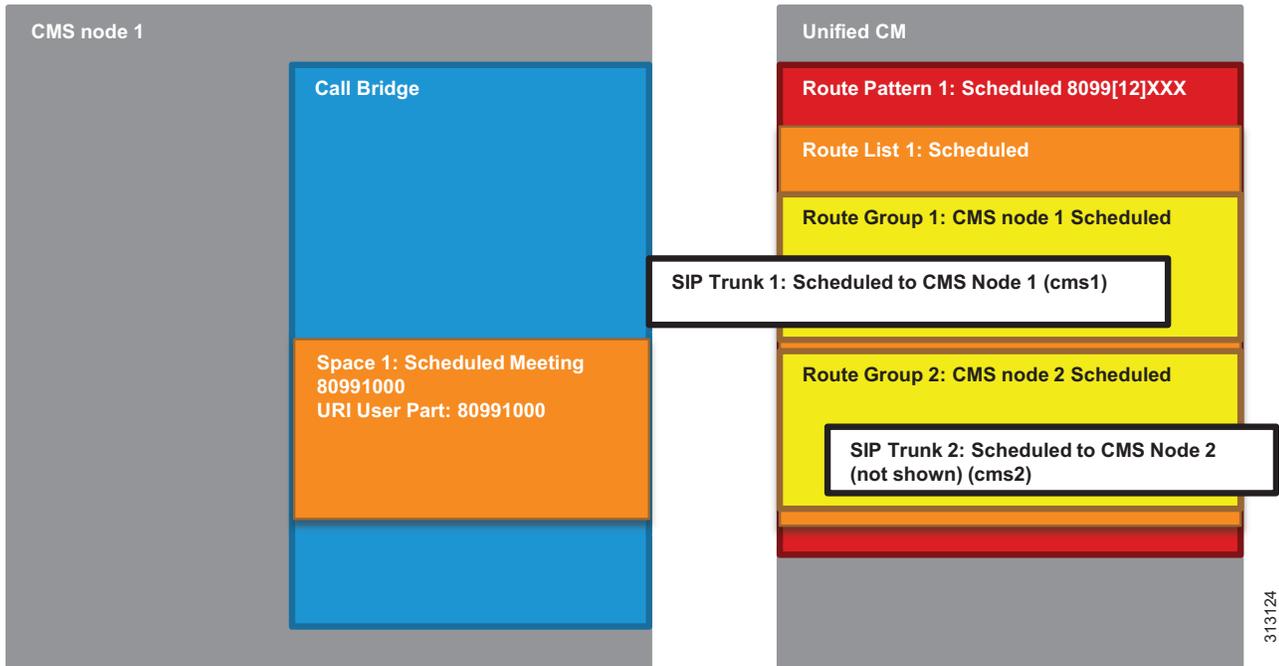
無期限会議とスケジュール済み会議は、インスタント会議と同様の方法で Unified CM で設定されますが、メディア リソースではなくダイヤルプランを設定する必要があります (C : 図 3-15)。無期限会議およびスケジュール済み会議には、インスタント会議用に作成したのと同じ SIP トランクと SIP プロファイルを使用しますが、C : 表 3-17 に示す設定値を使用します。

C : 図 3-15 Cisco Unified CM と Cisco Meeting Server スペースのスケジュール済み関係



313123

C : 図 3-16 無期限会議とスケジュール済み会議用の Cisco Unified CM の設定



インスタント会議用に作成されたすべての SIP トランク用のルート グループを作成します。ルート グループをルート リストの中に追加します。コールがそのルート を指すルート パターンに一致する場合に、ルート リストが選択されます。

SIP トランクを介して Cisco Meeting Server にコールをルーティングするには、ルート リスト用のルート パターンを設定します。ルート パターンは、C : 表 3-18 に示すように、スケジュール済み会議用に設定されたエイリアス範囲と一致する必要があります。管理者が Cisco TMS でスケジュール済み会議の数値 ID 範囲を作成すると、スケジュール済み会議用のスペースが作成され、数値 ID ごとに 1 つのスペースが作成されます。詳細については、4. Cisco TelePresence Management Suite を展開するのセクションを参照してください。

C : 表 3-18 スケジュール会議ルート リストのルート パターン

パターン	パーティション	ゲートウェイまたはルート リスト	説明
8099[12]XXX	ESN	RL_SPACE_SCHED	スケジュール済みエイリアス範囲と一致するパターン

Cisco Meeting Server の無期限会議用の展開とルート パターン設定の詳細については、5. Cisco Meeting Server スペースを展開するのセクションを参照してください。

概要

上記の展開タスクを完了すると、Unified CM が Cisco Meeting Server と通信できるようになります。

4. Cisco TelePresence Management Suite を展開する

このセクションでは、Cisco Meeting Server を使用したスケジュール済み会議用の Cisco TMS の展開タスクについて説明します。

概要

Cisco TMS の高適用性のための展開タスク：

1. アクティブ ノードとパッシブ ノードで Cisco TMS をインストールして設定します。
2. ネットワーク ロード バランサ (NLB) をインストールして設定します。
3. アクティブ ノード サーバとパッシブ ノード サーバの間のファイル共有を設定します。

Cisco TMS の基本設定のための展開タスク：

4. Active Directory 統合、グループ構造、およびユーザを設定します。
5. TMS システム ナビゲータのフォルダ構造を作成します。
6. デフォルトの会議設定を行います。

スケジュール済み会議用の Cisco TMS の展開タスク：

7. Cisco Meeting Server と TMS を統合します。
8. Unified CM と TMS を統合します。
9. 会議室エンドポイントを TMS に追加します。
10. TMS Extension for Microsoft Exchange (TMSXE) をインストールして設定します。

Cisco TMS の高適用性のための展開タスク

このセクションでは、高可用性を備えた Cisco TMS を展開するために必要なタスクについて説明します。

アクティブ ノードとパッシブ ノードでの Cisco TMS のインストールと設定

次の場所にある最新版『Cisco TelePresence Management Suite Installation and Upgrade Guide』のガイドラインに従って、冗長展開用に Cisco TelePresence Management Suite (TMS) をインストールする必要があります。

<https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-installation-guides-list.html>

- プライマリ サーバにこのアプリケーションをインストールします。
- 計画段階で設定した外部 SQL リソースを指し示します。
- 暗号化キーをメモしておきます。
- Web ポータルにログインして TMS 冗長性を有効にし、基本的な操作を検証します。
- 1 番目のサーバの暗号化キーを使用し、1 番目のサーバと同じ SQL クレデンシャルを使用して、2 番目のサーバにアプリケーションをインストールします。

両方のサーバが、すべての会議データと設定データが保存されている 1 つの SQL データベースにアクセスします。アクティブ ノード設定とパッシブ ノード設定で、1 つの暗号化キーと証明書が両方のサーバに対して使用されます。この暗号化キーと証明書をそれぞれのサーバに配置しておくことで、エンドユーザから TMS への通信と、TMS から管理対象デバイスへの通信に、セキュアプロトコルを使用できるようになります。

ネットワーク ロード バランサ (NLB) のインストールと設定

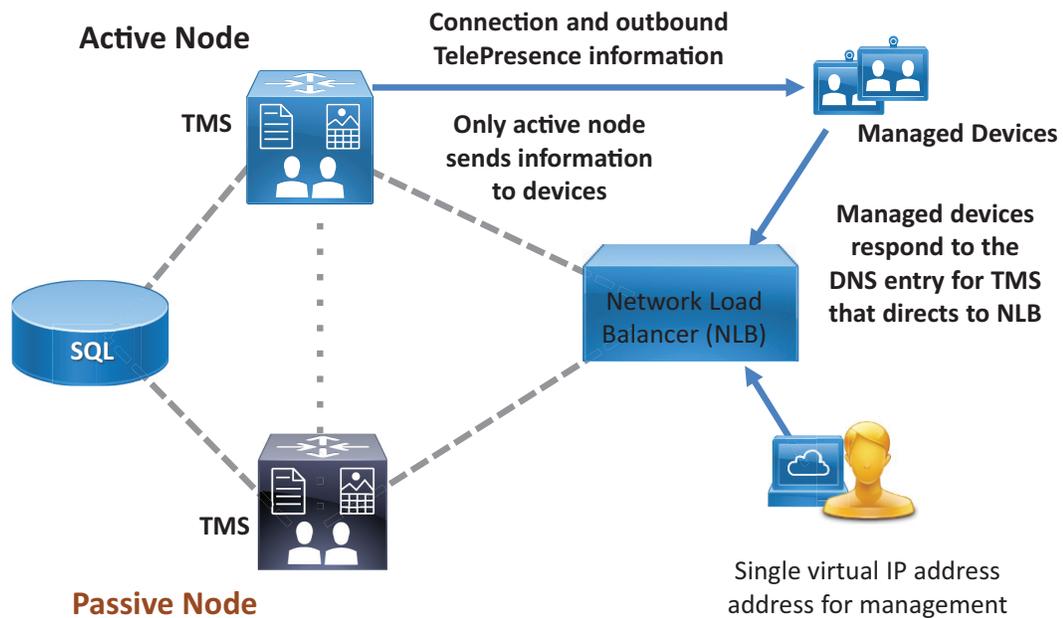
ネットワーク ロード 分散 設定の詳細は、お客様が選ぶロード バランサの指示に応じて異なります。以下は、設定する必要がある機能要件です。

- HTTP、HTTPS、および SNMP トラフィックをアクティブ ノードに転送します。
- Cisco TMS 内で Probe URL へのネットワーク ロード バランサ プロブを設定します。
- すべてのトラフィックをアクティブ ノードにプッシュします。

Cisco TMS サーバは発信通信を管理対象デバイスに直接送信し、トラフィックを NLB 経由でルーティングしません。ただし、管理対象デバイスからのすべての戻り通信とすべての Web ポータル要求は、NLB 経由でルーティングされる必要があります。通信パスにより、エンドユーザとエンドポイントは、どの TMS サーバ ノードがアクティブ モードであるかに関係なく、1 つのアドレスを使用できます。

TMS ネットワーク設定を、ネットワーク ロード バランサで設定されている TMS アドレスの FQDN に設定します。TMS 内のこの設定によって、管理対象デバイスが TMS との通信を開始するときに使用するアドレスが生成されます。ロード バランサに解決される tms.ent-pa.com の FQDN を使用することで、エンドポイントまたはエンドユーザ Web クライアントからのすべての着信トラフィックが NLB を経由して送信され、アクティブ ノードに解決されます (C : 図 3-17 を参照)。

C : 図 3-17 NLB による管理対象デバイスからアクティブ TMS ノードへの通信の指示



348936

アクティブ ノード サーバとパッシブ ノード サーバの間のファイル共有の設定

すべての運用データは SQL データベースに保管されますが、一部のアプリケーション固有ファイルはホスト サーバのファイル ストラクチャ内に保存されます。これらのカスタマイズ可能なファイルは TMS アプリケーションにより追加され、冗長環境を使用する場合は 2 つのサーバ間でこれらのファイルを同期する必要があります。このようなファイルには、Cisco TMS にアップロード可能なソフトウェアおよびイメージ、Cisco TMS により作成されたイメージなどが含まれます。

デフォルトのインストール環境では、ファイルの場所は次のとおりです。

C:\Program Files\TANDBERG\TMS\Config\System\

C:\Program Files\TANDBERG\TMS\Data\GenericEndpoint\

C:\Program Files\TANDBERG\TMS\Data\SystemTemplate\

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\CompanyLogo\

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\ExternalSourceFiles\

C:\Program Files\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware\

Windows Server オペレーティング システムの分散ファイル システム (DFS) を使用して、2 つのサーバ間のレプリケーション プロセスを実行します。「フル メッシュ」設定が使用されている場合、DFS は 2 つのサーバ間でこれらのファイルを同期した状態で維持します。

Cisco TMS の基本設定のための展開タスク

プリファードアーキテクチャで意図されているとおりに導入環境が機能するようにするには、Cisco TMS のインストール中に次の追加設定タスクを実行します。

- [Active Directory の統合、グループ構造、ユーザ](#)
- [システム ナビゲータ フォルダの構造](#)
- [デフォルトの会議設定](#)
- [デフォルトの会議設定](#)
- [TMS 内での電子メール テンプレートの変更](#)

Active Directory の統合、グループ構造、ユーザ

Active Directory サービス アカウントのすべての情報が正しく入力されていることを確認します。



注 AD 接続のすべての設定が正しいことを確認し、接続をテストします。AD 同期が機能していない場合でも、TMS 内でその他の AD インターフェイス コマンドを実行すると、エラーが表示されないことがあります。

Active Directory Group を使用して、組織のニーズに対応するグループ構造を作成します。

デフォルトでは、TMS のインストール中に 3 種類のグループが作成されます。

- Users
- Video Unit Administrator
- Site Administrator

顧客のニーズに対応するようにこれらのグループを変更できますが、削除はできません。デフォルトでは、すべてのグループに Site Administrator と同じアクセス権限が付与されます。

これらのデフォルトグループでのユーザ エントリは手動入力に限定されているため、グループを Active Directory からインポートし、既存の Active Directory グループを使用して TMS 機能へのエンドユーザ アクセスを管理する必要があります。会議をスケジュールするエンドユーザ用のグループに加えて、サポートデスク担当者や技術管理者用のグループも必ず考慮してください。

グループに関する追加情報については、次の場所にある『Cisco TelePresence Management Suite Administrator Guide』の最新版を参照してください。

<https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html>

[AD からインポート (Import from AD)] 機能を使用すると、エンドユーザの職務を一元的に管理できます。従業員を追加または削除するか、あるいは職務を変更して、組織的な Active Directory グループを変更すると、TMS 権限が自動的に更新されます。

Active Directory からグループをインポートしたら、各グループに適切な権限を割り当てます。表示される画面で、グループに設定しない権限をすべてオフにします。これらの権限を制限しないと、意図しない設定変更が発生する可能性があります。

また、すべてのユーザに対して適切なデフォルトグループを選択してください。



注

Cisco CMS にアクセスできるすべてのユーザは自動的に Users グループに追加されます。このグループをオフにすることはできません。管理者が組織内のすべてのユーザに対して付与しない権限があれば、それらをすべて選択解除します。

ユーザのインポート

グループの権限が設定されたら、[すべてのユーザを AD と同期する (Synchronize All Users with AD)] 機能を使用してユーザをインポートします。組織の規模と関連するグループの数に応じて、同期が完了するまでに長時間かかることがあります。



注

ユーザは、初めて TMS にログインするまではユーザ リストに表示されません。

システム ナビゲータ フォルダの構造

TMS システム ナビゲータは、フォルダ構造を使用して管理者のためにデバイスを論理的にグループ化します。組織の物理的な環境に対応したフォルダ構造を作成します。これらのフォルダは管理者に対してだけ表示され、エンドユーザに対しては表示されません。組織の論理フローに基づいてフォルダを配置します。たとえば、地域ごとに 1 つのフォルダを作成し、続いてインフラストラクチャのサブフォルダと会議室エンドポイントのための別のフォルダを作成します。システム ナビゲータ内のフォルダには、TMS から接続の指示を受信するインフラストラクチャ デバイスまたはエンドポイント、あるいはこの両方を含めることができます。

デフォルトの会議設定

会議をスケジュールする前に、管理者はエンドユーザ コミュニティの使用モデルと、エンドポイントの制限について理解しておく必要があります。検討すべき重要な Cisco TMS 設定には、次のものがあります。

- [ワンボタン機能](#)
- [帯域幅](#)
- [参加者に対し 5 分前の接続を許可する](#)

ワンボタン機能

ワンボタン機能により、エンドユーザは特定のルームで開催される当日の会議をカレンダーで確認し、会議への接続を開始できます。Cisco TMS はユーザに対し、1 要求あたり 72 時間分のカレンダー情報を提供します。

帯域幅

この設定はエンドポイントごとに行います。ネットワークに必要な設定にあわせて帯域幅を調整してください。コンテンツの HD メインチャネルと最大解像度を可能にするには、非ルームシステムのビデオデバイスのデフォルト帯域幅を 2048 kbps に設定する必要があります。最大帯域幅にこれよりも低い値が設定されているエンドポイントはすべて、その最大帯域幅で接続します。

参加者に対し 5 分前の接続を許可する

エンドユーザの時間インターフェイスで多少の差異を許可するには、この設定を選択します。TMS サーバでの正確な時刻よりも前にユーザが接続できるようにすることで、より一貫性のあるエンドユーザエクスペリエンスを提供し、また会議開始時刻の数分前にエンドユーザが会議に接続しようとしたときに「接続できない」というメッセージが表示されなくなります。

TMS 内での電子メール テンプレートの変更

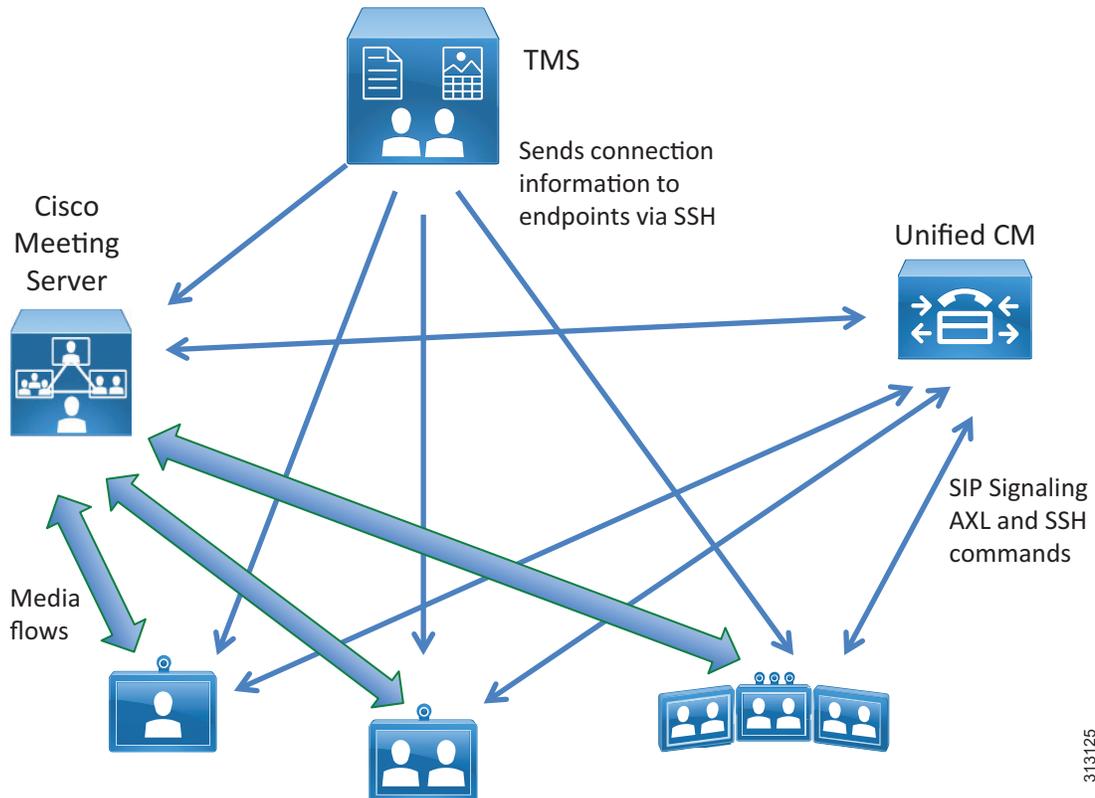
Cisco TMS には、会議主催者への通知に使用できるテンプレートがあります。ただし Cisco TMSXE では、Cisco TMS が送信する電子メールのメッセージにエラー、警告、および情報テキストが挿入されることがあります。管理者はこれらのメッセージを変更できます。{MEETING_TITLE}、{CONTACT_HOST} のように中カッコで囲まれたテキストは、スケジュール済みイベントの特定のコンテンツを組み込む変数であるため、これらのテキストを削除または変更しないようにしてください。

すべての電子メール テンプレートで、TMS により自動生成される通信内容が目的の手續きに対応していることを確認します。多くのテンプレートはシンプルに作られており、各組織がテンプレートを拡張することを前提としています。また、テンプレートは標準 HTML エディタを使用して変更できます。

スケジュール済み会議用の Cisco TMS の展開タスク

Cisco TMS がスケジュール済み会議を作成できるようにするため、必要なコンポーネントを TMS にシステムとして追加する必要があります。TMS スケジューリングメカニズムがすべてのデバイスのコール制御エンティティを認識できるようにするため、Unified CM が TMS に追加されます。TMS は Unified CM の設定を制御しませんが、Unified CM が管理する会議室のエンドポイントと直接通信します。(C : 図 3-18 を参照)。

C : 図 3-18 Cisco TMS と Unified CM 管理対象エンドポイントの直接通信



313125

Cisco Meeting Server と Cisco TMS の統合

Cisco TMS でスケジュール済み会議のスケジューリングと会議制御を可能にするには、各 Cisco Meeting Server クラスタから 1 つの Cisco Meeting Server ノードを追加します。

特定の範囲の数值 ID を使って Cisco TMS を設定する必要があります。これらの ID は、スケジュール済みコールの配置場所を決定するために Cisco TMS で使用されます。

各 Cisco Meeting Server クラスタから 1 つの Cisco Meeting Server を Cisco TMS に追加します。それらを該当するフォルダに追加します。その際、Cisco Meeting Server で設定された管理者アカウントを使用します。Cisco TMS で設定された TelePresence Conductor ごとに、C : 表 3-19 に示すパラメータを設定します。

C : 表 3-19 Cisco Meeting Server 用の Cisco TMS パラメータの設定

設定	値	コメント
[IP アドレス (IP Address)]	10.X.X.2:445	Cisco Meeting Server Web 管理インターフェイスの IP アドレスとポート番号
[ユーザ名 (Username)]	[TMSadmin]	この設定は、Cisco Meeting Server で設定されたユーザ名と一致する必要がある
[パスワード (Password)]	<パスワード>	
[使用タイプ (Usage Type)]	[その他 (Other)]	

Cisco Meeting Server を追加した後、C : 表 3-20 に示すように、Cisco Meeting Server 設定の中で代替 IP ネットワーク設定を指定します。最初の Cisco Meeting Server で障害が発生すると、代替 IP Cisco Meeting Server が操作を引き継ぎます。

C : 表 3-20 Cisco Meeting Server 用の代替 IP ネットワーク設定

設定	値	コメント
[代替 IP (Alternate IP)]	< ドロップダウンで 1 つ選択 >	Call Bridge が有効になっている Cisco Meeting Server クラスタ ノード
[代替 IP ユーザ名 (Alternate IP Username)]	[TMSadmin]	代替 IP アドレスで指定された IP アドレスを持つ Cisco Meeting Server で設定されたユーザ
[パスワード (Password)]	<パスワード>	

会議エイリアスを設定し、ダイヤルプランの一環として Cisco Meeting Server で使用する、SIP トランクで指定される数値範囲を特定します。C : 表 3-21 は、スケジュールされたコール用の数値 ID 範囲を指定するための Cisco Meeting Server の拡張設定を示しています。

C : 表 3-21 Cisco Meeting Server の拡張設定

パラメータ	値
[ドメイン (Domain)]	Cisco Meeting Server に関連付けられたドメイン。
[数字 ID ベース (Numeric ID Base)]	これは、ダイヤルプランのスケジュール会議範囲の 1 番目の数字です。
[数字 ID の桁数 (Numeric ID Quantity)]	スケジュール済み会議に必要な数値 ID の数を指定します。

Cisco Meeting Server を追加するための設定を保存します。数値 ID ごとに、Cisco TMS は、Cisco Meeting Server 上の URI ユーザ部分として数値 ID を使って非アクティブスペースを作成します。これらのスペースは、Cisco TMS で作成されるスケジュール済み会議をホストするために使用されます。スケジュール済み会議を開始する時間になると、Cisco TMS は Cisco Meeting Server 上のスペースをアクティブにして、参加者がコールインを開始できるようになります。

Cisco TMS は、E.164 エイリアスと SIP URI の両方に、前述のステップで指定したダイヤルプランの数値を取り込みます。ただし TMS 内での E.164 ロジックの実装は、プリファードアーキテクチャのその他の場所での E.164 の使用方法とは異なります。TMS は E.164 エイリアスを H.323 通信だけに関連付けます。したがって、Cisco Meeting Server の特定の警告を無視するように TMS の統合チケットシステムを調整する必要があります。

Cisco Meeting Server が TMS に追加されたら、[ゲートキーパーモードオフ (Gatekeeper Mode Off)] 用のフィルタを追加することにより、このエントリのチケットフィルタを調整します。

スケジュールされたコールに Cisco Meeting Server を使用するには、Cisco TMS 内の Cisco Meeting Server 設定を編集する必要があります。H.323 ダイアルは両方向で無効、[予約の許可 (Allow booking)] は有効、SIP ダイアルは両方向で有効にする必要があります。

使用する数値 ID 範囲を設定する際には、スケジュール済み会議の番号範囲が Unified CM で設定されたものと一致するようにする必要があります。C : 表 3-22 に示すように、Cisco TMS 内で Cisco Meeting Server の拡張設定を編集します。ドメインは、Cisco Meeting Server で設定された XMPP ドメインと一致する必要があります。数値 ID は、Unified CM から Cisco Meeting Server へのトランク用に設定されたルートパターンと一致する必要があります。

C : 表 3-22 Cisco Meeting Server の拡張設定

設定	値	コメント
ドメイン (Domain)	cms.ent-pa.com	スケジュール済み会議の SIP URI ドメイン
[数字 ID ベース (Numeric ID Base)]	80991000	スケジュール済み会議にダイヤルインする参加者によって使われるダイヤル文字列を形成するために Cisco TMS で使用する最初の番号 (80991000 など)。
[数字 ID の桁数 (Numeric ID Quantity)]	1999	Cisco TMS が [数字 ID ベース (Numeric ID Base)] からの数値を増やす回数。この数値は、最大値がスケジュールに割り当てられた範囲を超えないように設定する必要があります (80991000 ~ 80992999)。

スケジュールリングに Cisco Meeting Server を使用するように Cisco TMS を設定することが重要です。そうしなければ、スケジュールリングが失敗します。[管理ツール (Administrative Tools)] > [設定 (Configuration)] > [会議設定 (Conference Settings)] で、C : 表 3-23 に示されているように設定を編集します。

C : 表 3-23 Cisco TMS Conference 設定

設定	値	コメント
[ルーティングの優先 MCU タイプ (Preferred MCU Type in Routing)]	Cisco Meeting Server	スケジュールリングに関して、他のデバイスより Cisco Meeting Server を優先する

Unified CM と TMS の統合

Unified CM はその他のすべての設定および管理の面で会議室のエンドポイントを管理しますが、予約と接続開始を実行できるようにするため、Unified CM クラスタを TMS に追加する必要があります。Unified CM を TMS に追加するには、次のタスクを実行します。

- Unified CM 内での Cisco TMS のアプリケーション ユーザの作成
- ご使用の環境での各 Unified CM クラスタのパブリッシャの追加

複数の Unified CM クラスタを追加する場合は、[コール制御](#)の章で説明するダイヤルプラン設定に準拠する必要があります。

Unified CM 内での Cisco TMS のアプリケーション ユーザの作成

このアプリケーション ユーザにより、Unified CM が制御するエンドポイントと TMS が通信できるようになります。このユーザには、Unified CM 内のスケジュール対象の会議室デバイスすべてを割り当てる必要があります。また、次のロールが設定されている Cisco TMS 専用のユーザグループにこのユーザを追加する必要もあります。

- Standard AXL API Access
- Standard CTI Enabled
- Standard SERVICEABILITY
- Standard CCM Admin Users
- 標準 RealtimeAndTraceCollection

詳細については、次の場所にある『*Administration Guide for Cisco Unified Communications Manager and IM and Presence Service*』の最新版を参照してください。

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

ご使用の環境での各 Unified CM クラスタのパブリッシャの追加

Unified CM パブリッシャを TMS に追加すると、TMS はそのエンドポイントのコール制御権限を認識します。Unified CM を認識しない場合、TMS スケジューリング エンジン は導入環境の全機能を利用できず、接続が失敗することがあります。

他のデバイスの場合と同じ方法でパブリッシャを追加します。TMS から入力を求められたときのユーザ名およびパスワードとして、上記ステップで作成したアプリケーション ユーザを使用します。

TMS への会議室エンドポイントの追加

IP アドレスまたは DNS 名でデバイスを追加する代わりに、[リストから (From List)] タブを使用して、Unified CM を選択します。TMS のスケジューリング インターフェイスから使用できるようにする会議室の TelePresence デバイスをすべて選択します。Unified CM の各エンドポイントの DN が、[コール制御](#) の章に記載されている E.164 ガイドラインに準拠していることを確認します。

TMS Extension for Microsoft Exchange のインストールと設定

Cisco TelePresence Management Suite Extension for Microsoft Exchange (Cisco TMSXE) は、Microsoft Outlook からビデオ会議のスケジュールを可能にする Cisco TelePresence Management Suite の拡張機能であり、Cisco TMS 会議を Outlook の会議室予定表にレプリケートします。

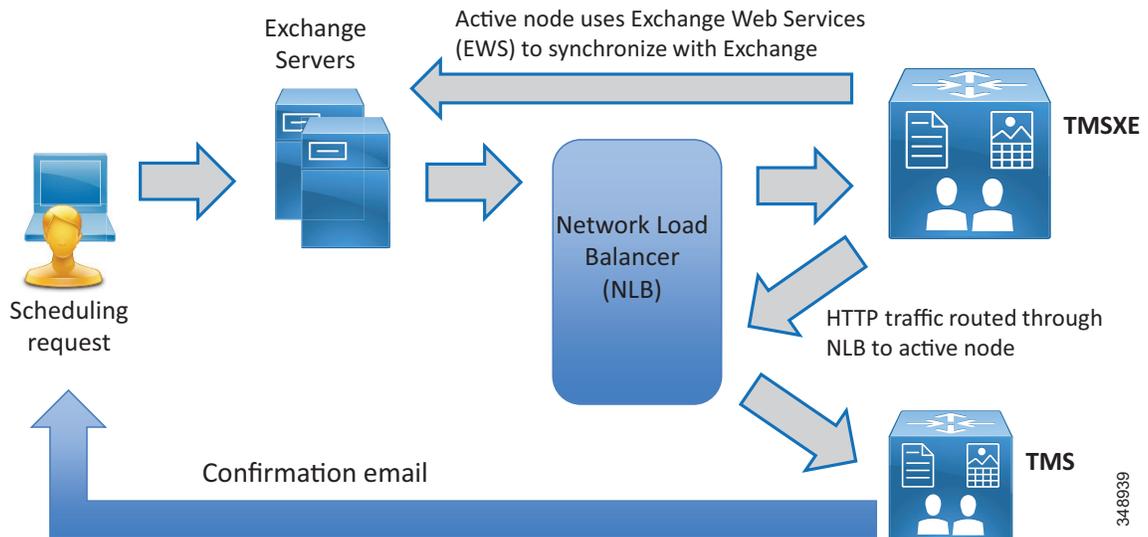
この TMS ソフトウェア拡張機能を使用するには、TMS 内で機能を有効にするためのライセンスキーが必要です。TMSXE ソフトウェアのインストール前に、このキーを TMS にインストールしておく必要があります。スケジュールされるエンドポイントの数が 50 を超える導入環境では、TMSXE を専用のサーバまたは仮想マシン インスタンスにインストールする必要があります。

前提条件

Cisco TMSXE をインストールする前に、Outlook と Exchange がすでにセットアップされており、ユーザがルーム メールボックスを含む会議を予約できることを確認してください (C : 図 3-19 を参照)。この統合は、エンドポイントグループによりライセンスされるか、または Application Integration ライセンス キーとしてライセンスされます。インストールを続行する前に、正しいキーを作成し、TMS に入力する必要があります。両方のオプションキーを追加した場合、Cisco TMS は Application Integration Package オプションのみを使用します。

Cisco TMSXE が使用できる Microsoft Exchange リソースは、オンプレミス、Office 365 ホスティング導入環境、または顧客のハイブリッド導入環境のいずれかです。お客様の特定の環境に適用される可能性のある推奨事項またはガイドラインについては、Microsoft Exchange の管理と導入に関する資料を参照してください。

C : 図 3-19 エンドユーザによる会議のスケジュールフローの例



システム別のオプション キーを Cisco TMS で有効化したら、[リモート予約を許可する (Allow Remote Bookings)] 設定により、各システムがライセンスを使用するかどうかが決まります。この設定により、エンドユーザが予約でき、個別のエンドポイント ライセンスの 1 つを使用できるエンドポイントを管理者が選択できます。Application Integration Package オプションを使用する場合は、この設定は無効であり非表示になります。

Cisco TMSXE にエンドポイントを追加するには、その前に、Exchange でこれらのエンドポイントがルーム メールボックスによって示されている必要があります。TMSXE のセットアップを簡素化するため、エンドポイントの Cisco TMS 表示名をメールボックス名として使用することを推奨します (スペースはすべて削除してください)。これにより、エンドユーザに対するシステム名の表示方法すべてで統一が図られます。

Exchange のプライバシー機能に関する特別な注意事項

Cisco TMSXE に追加されるすべてのルーム メールボックスが、予約件名とプライバシー設定を同一の方法で処理するように設定されている必要があります。つまり、以下の設定をすべてのメールボックスに適用するか、またはどのメールボックスにも適用しないかのいずれかになります。

- [件名の削除 (Delete the subject)]
サポート担当者が会議制御センターで特定の会議を識別できるようにするため、この機能を使用しないことを推奨します。また、これにより会議のタイトルが対応エンドポイントの One Button to Push インターフェイスに表示されるようになります。
- [開催者名を件名に追加する (Add the organizer's name to the subject)]
この設定を使用するには十分に注意し、組織の慣習に基づいて使用してください。あるユーザが複数グループの会議をスケジュールすると、スケジュールされた会議は会議の件名ではなくそのスケジュール担当者のユーザ名でリストされることに注意してください。会議

の件名の方が便利である可能性があります。一方、会議がそれぞれ該当する主催者によってスケジュールされる場合、特定の会議の件名を覚えておくよりも、「ボブの会議」と確認できる方が容易なことがあります。ほとんどの組織ではこの設定を使用しないことを推奨します。

- [承諾した会議に設定されたプライベートフラグを削除する (Remove the private flag on an accepted meeting)]
「プライベート」フラグは Outlook クライアント内では反映されますが、Cisco TMS ではサポートされていないため、会議の議題は以下の場所で制限なしで表示されます。
 - Cisco TMS 内
 - 組織内で件名を公開すべきではない会議に使用する会議室を、他の担当者も使用している場合は、会議室予定表をサポートしているエンドポイント。(たとえば、最高責任者による「合併会議」がスケジュールされている会議室を使用する、保留中の合併について知る必要がない下位レベルの従業員に対し、会議室システム予定表にこの会議が表示されることがあります。)
 - Exchange で「プライベート」フラグが設定されている予約の参加者または定例会議パターンが Cisco TMS で変更されると、この変更が Exchange にレプリケートされる時点で「プライベート」フラグが削除されます。

TMSXE ユーザの作成

- Active Directory で TMSXE ユーザを作成し、TMS にインポートします。
- TMS では、[予約 (Booking)] の下で次の権限が有効な既存のグループまたは新規のグループにこのユーザが属している必要があります。
 - [読み取り (Read)]
 - [更新 (Update)]
 - [代理予約 (Book on Behalf of)]
 - [会議承認 (Approve Meeting)]

証明書のインストール

Cisco TMSXE と TMS の通信には HTTPS が使用されます。TMSXE サーバと Exchange 環境間のセキュア通信は証明書でも可能です。TMS アプリケーションサーバと同様に、TMSXE のアクティブ ノードとパッシブ ノードの両方に同じ証明書がロードされ、証明書の DNS 項目は TMSXE に使用されるネットワーク ロード バランサのアドレスの項目を指し示します。

ソフトウェア インストーラの実行

- TMS Booking Service を選択します。
- アクティブ ノードまたはパッシブ ノードに適切な冗長性オプションを選択します。
- アクティブ ノードとパッシブ ノードの両方でソフトウェア インストールを実行します。

アクティブ ノードとパッシブ ノードの両方でインストールが完了したら、各ノードのプロンプト URL を使用してネットワーク ロード バランサを設定します。

Cisco TMSXE の設定

- Cisco TMS 接続情報
TMSXE アプリケーションが TMS アプリケーションと通信できるようにするため、Active Directory で作成した TMSXE アカウントを使用して TMS 接続情報を設定します。

- Exchange Web Services の設定
ユーザとリソース メールボックスのために TMSXE が Exchange サーバと通信できるように Exchange Web Services (EWS) を設定します。この接続に使用するクレデンシヤルは、他の場所で使用されるものと同じ TMSXE クレデンシヤルです。
- Exchange と TMS リソースの調整
TMS システム ID に合わせて Exchange リソースを調整します。この操作を個別に行うことも、あるいは次の場所にある『Cisco TelePresence Management Suite Extension for Microsoft Exchange Deployment Guide』の最新版に記載されている .csv ファイルを使用することもできます。

<https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-extensions/products-installation-guides-list.html>

概要

上記の展開タスクを完了すると、スケジュール済み会議用の Cisco Meeting Server と通信するように Cisco TMS が設定されます。

5. Cisco Meeting Server スペースを展開する

このセクションでは、Cisco Collaboration Meeting スペースを展開するために必要な主なタスクについて説明します。

概要

Cisco Meeting Server 常設会議用の統一された CM の展開タスク :

1. Unified CM と Cisco Meeting Server の間の Early Offer SIP トランクを設定します。以前に設定した SIP トランク SIP_TRUNK_CMS1 をここで使用することができます。
2. 関連するトランクを含むルート リストを指し示すスペース数字エイリアス用の新しいルート パターンをセットアップします。以前に設定したルート リスト RL_SPACE_SCHED をここで使用することができます。
3. タスク 2 で使用したルート リスト (RL_SPACE_SCHED) を指し示すスペース URI 用の SIP ルート パターンを作成します。

スペースを作成するための Cisco Meeting Server の展開タスク :

4. ユーザ プロファイルを作成し、マルチパーティ ランセンスをユーザに割り当てます。
5. LDAP からユーザをインポートし、スペースを作成します。
6. 着信コールを処理するダイヤル プラン ルールを作成します。

展開の考慮事項

Cisco Meeting Server スペースは、企業のデータセンターに配置された TelePresence インフラストラクチャで作成される無期限会議に似ています。各スペースには、会議を開始するためにユーザがいつでも発信できるビデオ アドレスの固有のセットが存在します。これらのビデオ アドレスは、数字エイリアスまたは SIP URI の形式で指定できます。各スペースを個別ユーザに関連付け、LDAP ユーザ同期を介して作成することができます。

Cisco Meeting Server スペースは、居場所に関係なく、参加者が会議に参加するための簡単な方法を提供します。すべてのユーザは、ラップトップ、テレプレゼンス会議室、デスクトップ エンドポイント、またはモバイルデバイスから同じ仮想会議室にダイヤルします。

スペースを展開するには、Unified CM と Cisco Meeting Server の展開が必要です。以降のセクションでは、スペースの各コンポーネントの展開に関するプロセスの概要を説明します。



Tip

スペースを展開する前に、会議エイリアスの形式（数字または SIP URI）を決定します。

Cisco Meeting Server 常設会議用の統一された CM の展開タスク

Unified CM の主な機能は、Cisco Meeting Server との間のコールルーティングを処理することです。Early Offer 用に有効にされた SIP トランクを使用して、Unified CM を Cisco Meeting Server に接続します（以前にスケジュール済み会議用に設定したものと同一トランク SIP_TRUNK_CMS1 を使用します）。ユーザがスペース エイリアスにダイヤルすると、コールは SIP トランクを介して Cisco Meeting Server 上の Call Bridge に送信されます。同様に、Cisco Meeting Server は、自動ダイヤル参加者用の SIP トランクを介して Unified CM にコールを送信できます。会議エイリアスには、2つの形式（SIP URI と数字）があります。ダイヤルプラン設計には、スペースの数字エイリアスと SIP URI の両方のコールルーティングを含める必要があります。ダイヤルプラン設計の詳細については、[コール制御](#)の章を参照してください。

Cisco Meeting Server スペースを個別のユーザごとに作成でき、ユーザの DID 番号に基づくスペース数字エイリアスにすることができます。C : 表 3-24 は、[コール制御](#)の章のダイヤルプラン例を使用した展開用のスペース数字エイリアス範囲を示しています。

C : 表 3-24 スペース数字エイリアスの範囲

サイト	+E.164 DID 範囲	スペース数字エイリアスの範囲
SJC	+1 408 555 4XXX	8-004-4XXX
RTP	+1 919-555 1XXX	8-005-1XXX
RCD	+1 972 555 5XXX	8-006-5XXX

数字エイリアスでは、C : 表 3-25 に示すように、無期限会議用の Cisco Meeting Server ルートリストにルーティングする各サイトのルートパターンを設定します。

C : 表 3-25 スペース数字エイリアスのルートパターン設定

パターン	パーティション	ゲートウェイまたはルートリスト	説明
80044XXX	ESN	RL_SPACE_SCHED	SJC DID 範囲に一致するパターン
80051XXX	ESN	RL_SPACE_SCHED	RTP DID 範囲に一致するパターン
80065XXX	ESN	RL_SPACE_SCHED	RCD DID 範囲に一致するパターン

SIP URI では、ドメイン部分として XMPP ドメインを使用します。このドキュメントで設定する XMPP ドメインは cms.ent-pa.com です。たとえば、参加者は <username>.space@cms.ent-pa.com にダイヤルして Cisco Meeting Server 上の会議に参加することができます。また、Cisco Meeting アプリのユーザは、統一された CM 登録デバイスなどから、たとえば <ユーザ名>@cms.ent-pa.com にダイヤルすることによっても到達できます。

Unified CM は、XMPP ドメインに関するすべてのコールを Cisco Meeting Server に送ります。
C : 表 3-26 に示すように、無期限会議用の Cisco Meeting Server ルートリストにコールをルーティングする Cisco Meeting Server XMPP ドメインを含むドメインルーティング SIP ルートパターンを設定します。

C : 表 3-26 スペース URI 用の SIP ルート パターンの設定

パターン	パーティション	ゲートウェイまたはルート リスト
cms.ent-pa.com	URI	RL_SPACE_SCHED

スペースを作成するための Cisco Meeting Server の展開タスク



注

このセクション内のタスクは、REST API を実行するためのツール (Postman など) と Cisco Meeting Server API を使用して展開されます。API の詳細については、<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html> にある『Cisco Meeting Server API Reference Guide』の最新版を参照してください。

Cisco Meeting Server で会議をホストするには、その前にマルチパーティ ライセンスを適用する必要があります。Personal Multiparty Plus (PMP+) が必要な場合は、ユーザごとにライセンスを付与する必要があります。PMP+ を割り当てるには、hasLicense フィールドが **true** に設定されたユーザ プロファイル オブジェクトにユーザを関連付ける必要があります。HasLicense フィールドが **false** の場合またはユーザ プロファイル オブジェクト内に存在しない場合は、ユーザがライセンスを持っていないため、Shared Multiparty Plus (SMP+) が使用されます。ユーザ プロファイルは、ユーザの機能を指定します。API を使用して、**C : 表 3-27** に示すパラメータを使って userProfile オブジェクト (POST /userProfiles) を作成し、hasLicense フィールドを **true** に設定します。

C : 表 3-27 userProfile オブジェクトのパラメータ

パラメータ	値	説明
hasLicense	true	Personal Multiparty ライセンスを使用する
canReceiveCall	true	Cisco ミーティング アプリのユーザにコールの受信を許可する

Cisco Meeting Server 内のすべてのユーザは LDAP ディレクトリに存在します。(以前に作成した) ユーザ プロファイル オブジェクトをパラメータの 1 つとして使用し、ディレクトリから Cisco Meeting Server にユーザを同期する必要があります。インポートされたすべてのユーザはそのユーザ プロファイルに関連付けられます。ユーザ同期プロセスを作成するには ldapServers、ldapMappings、および ldapSources オブジェクトが必要です。

ldapServers は、サーバにアクセスするための場所、クレデンシャル、その他の属性を指定します。**C : 表 3-28** に示すパラメータを使用して、ldapServers オブジェクト (POST /ldapServers) を作成します。

C : 表 3-28 ldapServers オブジェクトのパラメーター

パラメータ	値の例	説明
address	10.192.168.10	ディレクトリの IP アドレスまたは FQDN
portNumber	636	ディレクトリによって使用されるポート番号
username	ent-pa\tmssvc	ディレクトリにアクセスするためのユーザ名

C : 表 3-28 *ldapServers* オブジェクトのパラメーター (続き)

パラメータ	値の例	説明
password	<パスワード>	ユーザ名に関連付けられたアカウントのパスワード
secure	true	ディレクトリ アクセスにセキュア接続を使用する

ldapMappings ではスペースに関する属性 (名前、ユーザ名、URI など) を指定できます。これらの属性は、Microsoft Active Directory からの属性に基づいて作成できます (C : 表 3-29 を参照)。C : 表 3-29 に示すパラメータを使用して、*ldapMappings* オブジェクト (POST /*ldapMappings*) を作成します。

C : 表 3-29 *ldapMappings* オブジェクトのパラメータ

パラメータ	値の例	説明
nameMapping	\$displayName\$	表示名
jidMapping	\$sAMAccountName\$@cms.ent-pa.com	XMPP ユーザ名
coSpaceNameMapping	\$displayName\$ のミーティング スペース	スペース名
coSpaceUriMapping	\$sAMAccount\$.space	スペース プライマリ URI
coSpaceSecondaryUriMapping	80044 \$ telephoneNumber %. * ([[d igit:]] {3}) \$^ 1/ \$	スペース セカンダリ URI

スペース セカンダリ URI のプレフィックスはサイトによって異なり、最後の 3 桁がユーザの DID 番号から抽出されることに注意してください。コール制御 の章のダイヤルプラン例に従うと、SJC サイトにはプレフィックス 80044、RTP サイトにはプレフィックス 80051、RCD サイトにはプレフィックス 80065 がそれぞれ付加されます。したがって、*ldapMappings* オブジェクトはサイトごとに 1 回ずつ、合計 3 回作成されます。

C : 表 3-29 のマッピングを使用してユーザをインポートすると、ユーザに <username>@cms.ent-pa.com というユーザ名が付きます。Cisco ミーティング アプリにサインインするときにこれを使用できます。ユーザに、プライマリ URI <username>.space@<domain> とセカンダリ URI 80044XXX@<domain> に関連付けられたスペースが割り当てられます。ドメインは、Cisco Meeting Server 内の着信コール用の呼一致表で設定されたドメイン名に基づきます (C : 表 3-31 を参照)。

特定のユーザ グループを Cisco Meeting Server にインポートできるように、LDAP ソースを使用して LDAP サーバ、LDAP マッピング、ユーザ プロファイル、および LDAP フィルタが単一のソースに結合されます。C : 表 3-30 に示すパラメータを使用して、*ldapSources* オブジェクト (POST /*ldapSources*) を作成します。

C : 表 3-30 *ldapSources* オブジェクトのパラメータ

パラメータ	値の例	説明
server	< <i>ldapServers</i> id>	<i>ldapServers</i> オブジェクト ID
mapping	< <i>ldapMappings</i> id>	<i>ldapMappings</i> オブジェクト ID
userProfile	< <i>userProfile</i> id>	<i>userProfile</i> オブジェクト ID
baseDn	ou=enterprise,dc=ent-pa,dc=com	トップ レベル検索ベース
filter	memberof=cn=sjcgroup,ou,ou=enterprise,dc=ent-pa,dc=com	LDAP フィルタ

GET 操作を使用してオブジェクトの ID を取得できることに注意してください。たとえば、ldapMapping オブジェクトの ID を取得するには GET /ldapMappings を使用します。また、ユーザが属する Active Directory グループに基づいて各サイトのユーザがインポートされるように、サイトごとに異なるフィルタが存在します。たとえば、SJC ユーザは **sjcgroup** Active Directory グループに、RTP ユーザは **rtpgroup** Active Directory グループに、RCD ユーザは **rcdgroup** Active Directory グループに属する必要があります。そのため、サイト固有の ldapMapping とフィルタを使用して 3 つの ldapSource オブジェクトが作成されます。

すべての LDAP ソースが作成された後、ldapSyncs オブジェクト (POST /ldaySyncs) を使用して、ただちにユーザ同期を開始します。同期が完了したら、すべてのサイトのユーザと、インポートされたユーザごとのスペースが Cisco Meeting Server に作成されるはずですが。



注 Cisco ミーティング アプリでユーザが手動でスペースを作成することも、API を使ってスペースを作成することもできます。

次に、Cisco Meeting Server で着信コールを処理するダイヤルプランルールを作成します。いずれかの Web 管理インターフェイスを参照し、C : 表 3-31 の値を使用して、Web インターフェイス ([設定 (Configuration)] -> [着信コール (Incoming Calls)]) で設定された着信コールの呼一致表にドメインを追加します。ドメインは、XMPP ドメイン (cms.ent-pa.com)、トップレベルドメイン (ent pa.com)、およびすべての Call Bridge の FQDN および IP アドレス (us-cms1.ent-pa.com と cms2.ent-pa.com) です。

C : 表 3-31 着信コール処理の設定

ドメイン名	プライオリティ	スペースを対象とする	ユーザを対象とする	IVR を対象とする	Lync を対象とする
cms.ent-pa.com	100	はい	はい	はい	いいえ (No)
ent-pa.com	100	はい	いいえ (No)	はい	いいえ (No)
us-cms1.ent-pa.com	100	はい	いいえ (No)	いいえ (No)	いいえ (No)
us-cms2.ent-pa.com	100	はい	いいえ (No)	いいえ (No)	いいえ (No)
10.x.x.60	100	はい	いいえ (No)	はい	いいえ (No)
10.x.x.61	100	はい	いいえ (No)	はい	いいえ (No)

XMPP ドメイン (cms.ent pa.com) にダイヤルされるすべての SIP URI コールは、スペース宛てまたは Cisco ミーティング アプリ ユーザ宛てです。数字ダイヤリングを使用してスペースを呼び出すユーザは、トップレベルドメインまたはコールブリッジ FQDN あるいは IP アドレスのルールにヒットします。数字ダイヤリングを使用した場合、Cisco ミーティング アプリのユーザには到達できません。

概要

上記の展開タスクを完了すると、ユーザは Cisco ミーティング アプリを使用してスペースにサインインし、PIN を指定したり、メンバーを追加したり、その他の環境設定をカスタマイズしたりできます。ユーザは SIP URI または数字エイリアスをダイヤルして会議を開始できます。

6. Cisco Meeting Management の展開

このセクションでは、Cisco Meeting Management スペースを展開するために主な展開タスクについて説明します。

概要

Cisco Meeting Management の展開タスク：

1. ワンタイムパスワードを使用して、初回セットアップを実行し、Cisco Meeting 管理ポータルにログインします。
2. ユーザ認証とグループ マッピングの LDAP セットアップを続行します。Cisco Meeting Server と同じディレクトリを使用します。
3. CDR 受信者、Cisco TMS、および NTP アドレスを設定します。Cisco Meeting Server と TMS に同じ NTP を使用して、すべてのタイムスタンプが同期していることを確認します。
4. Cisco Meeting Management に call bridge を追加します。

展開の考慮事項

Cisco Meeting Management は、ユーザ認証に LDAP ディレクトリを使用し、LDAP ディレクトリを通じてユーザ ロールを判別するユーザ グループをマッピングします。導入には少なくとも 2 つの LDAP ディレクトリグループが必要です。管理者用に 1 つのグループ (CMMAdmin など) と、ビデオオペレータ用に別のグループ (CMMOperator など) を作成します。次に、初期セットアップに進む前に、どのユーザがどのグループに所属するかを決定し、対応するグループにユーザを割り当てる必要があります。

Cisco Meeting Management の展開タスク

初期セットアップを開始し、ワンタイムパスワードを使用して初めて Cisco Meeting Management ポータルにログインするステップまで、続行します。初期セットアップの詳細については、以下で提供される最新バージョンの *Cisco Meeting Management インスタレーションおよび設定ガイド* を参照してください。

<https://www.cisco.com/c/en/us/support/conferencing/meeting-management/products-installation-guides-list.html>

Cisco Meeting Management のすべてのユーザは、会議管理がユーザ認証の判別に使用する LDAP ディレクトリに所属します。したがって、ポータルに初めてログインした後、**C : 表 3-32** の値を使用して LDAP サーバ、ユーザ検索ベース、および認証情報を設定します。

C : 表 3-32 サーバの初回設定

パラメータ	値の例	説明
LDAP サーバ：		
プロトコル	LDAPS	ディレクトリへのアクセスに使用するプロトコル
Server Address	10.192.168.10	ディレクトリの IP アドレスまたは FQDN
ポート	636	ディレクトリによって使用されるポート番号
検索ベース：		

C : 表 3-32 サーバの初回設定 (続き)

パラメータ	値の例	説明
Base DN	OU = Enterprise、DC = ent-pa、DC = com	トップレベルのユーザ検索ベース
属性の検索	sAMAccountName	ユーザの識別に使用される属性
Authorization:		
Bind DN	CN = tmssvc、OU = Enterprise、DC = ent-pa、DC = com	ディレクトリへのアクセスに使用するサービスアカウント
[パスワード (Password)]	<パスワード>	サービスアカウントのパスワード

Cisco Meeting Management では、LDAP グループを使用してユーザグループをマッピングするため、ポータルでユーザアクセス権限を決定します。この時点で、管理者に対して以前に作成した LDAP グループ (CMMGroup) をマッピングして、ユーザがログインしてセットアップを続行できるようにします。C : 表 3-33 に示される値を使用して、グループマッピングを設定します。

C : 表 3-33 グループマッピングの設定

パラメータ	値の例	説明
Group DN	CN = CMMAdmin、OU = Enterprise、DC = ent-pa、DC = com	管理者用の LDAP グループ

初期セットアップが完了したら、管理者 (CMMAdmin LDAP グループのユーザ) のいずれかの管理者の承認情報を使用して、Cisco Meeting Management ポータルにログインします。ログインしたら、設定 -> CDR に移動して、Cisco Meeting Management サーバの IP アドレスまたは FQDN (たとえば、https://10.x.x.68) を使用して CDR 受信者アドレスを設定します。Cisco Meeting Management は、このアドレスを使用して、コールブリッジに CDR 受信者 URI 文字列を作成して、コールに関連するイベントを受信します。次に、設定 -> TMS に移動し、TMS との Booking API 接続を設定して、今後予定されている会議に関する情報を取得します。設定には、C : 表 3-34 に示される値を使用します。

C : 表 3-34 TMS の設定

パラメータ	値の例	説明
ミーティング管理で TMS を使用する		TMS 統合を有効にする
TMS アドレス	10.x.x.75	TMS の IP アドレスまたは FQDN
プロトコル	HTTPS	TMS との接続に使用するプロトコル
ユーザ名	<username>	TMS サイト管理者のユーザアカウント
[パスワード (Password)]	<パスワード>	ユーザのパスワード

設定 -> NTP に移動して、NTP サーバを追加します。3 つのコンポーネント間で時刻を同期させるために、同じ NTP サーバを Cisco Meeting Server と TMS に使用する必要があります。

前述のとおり、Cisco Meeting Management には、管理者およびビデオ オペレータのユーザグループがあります。管理者グループは、初期セットアップ手順で追加されます。ビデオ オペレータはここで追加する必要があります。ユーザ -> ユーザ グループ に移動し、C : 表 3-35 に示される値を使用して設定を行います。

C : 表 3-35 ビデオグループの設定

パラメータ	値の例	説明
LDAP パス	CN = CMMOperator、OU = Enterprise、DC = ent-pa、DC = com	ビデオ オペレータの LDAP グループ
ロール	ビデオ オペレータ	ユーザ グループのロール

次に、モニタリングおよび管理のために、クラスタ内のすべてのコールブリッジを Cisco Meeting Management に追加します。サーバ ページに移動し、設定のための C : 表 3-36 の値を使用して、コールブリッジ（クラスタ内のすべてのユーザ）を追加します。

C : 表 3-36 コールブリッジの設定を追加する

パラメータ	値の例	説明
サーバーアドレス	10.x.x.60	コールブリッジの IP アドレスまたは FQDN
ポート	445	Cisco Meeting Server で webadmin が使用するポート
表示名	US-CMS1	コールブリッジを表す意味のある名前
ユーザ名	<user>	API アクセス権を持つローカル Cisco Meeting Server ユーザ
[パスワード (Password)]	<パスワード>	ユーザ パスワード

自動検出されたコールブリッジオプションを使用して、クラスタ内の他のコールブリッジを Cisco Meeting Management に追加します。Cisco Meeting Management では、スケジュールされた会議を表示するために、TMS に追加されたコールブリッジを把握しておく必要があります。そのためには、管理者が Cisco Meeting Server クラスタを TMS に関連付ける必要があります。クラスタ テーブルの上部に表示されるクラスタと TMS 設定の関連付け リンクをクリックし、C : 表 3-37 の値を使用して設定を行います。

C : 表 3-37 クラスタと TMS 設定の関連付け

パラメータ	値の例	説明
接続されているコールブリッジ	US-CMS1	TMS に追加されたコールブリッジの名前
TMS システム ID (TMS System ID)	<id>	TMS 内のコールブリッジの設定ページに表示される TMS ID

Cisco Meeting Management の 2 つ目のインスタンスで高可用性を実現する必要がある場合は、このセクションの作業を繰り返します。次に、ネットワークロードバランサーを 2 つの Cisco Meeting Management インスタンスの前に配置するように設定します。

概要

上記の設定作業が完了したら、ビデオ オペレータは Cisco Meeting Management ポータルにログインして、Cisco Meeting Server の会議をモニタおよび管理することができます。

関連資料

Cisco Meeting Server の追加情報については、下記リンクから入手可能な次のドキュメントの最新版を参照してください。

- Cisco Multiparty Licensing At-A-Glance
<https://www.cisco.com/c/dam/en/us/solutions/collateral/collaboration/pervasive-conferencing/at-a-glance-c45-729835.pdf>
- Cisco Meeting Server の導入ガイドと証明書のガイドライン ドキュメント
<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html>
- Cisco Meeting Server API Reference Guide
<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html>
- Cisco Meeting Server リリース ノート
<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-release-notes-list.html>