機能と追加構成

モバイルおよびリモートアクセスの基本設定が完了したら、この章を使用して MRA の機能とオプションの構成を構成します。

展開パーティション

展開は、ドメインと 1 つ以上の Unified Communications サービスプロバイダー (Unified CM、Cisco Unity Connection、IM and Presence Service ノードなど) を囲うために使用される抽象的な境界です展開を複数にする目的は、モバイルおよびリモートアクセス（MRA）ユーザーが使用できる Unified Communications サービスをパーティション化することです。よって、MRA ユーザーの異なるサブセットが同じ Expressway ペアを介してサービス一式にアクセスできます。

10 以上の展開はお勧めしません。

展開、関連ドメインおよびサービスは、Expressway-C で構成されます。

追加の展開を作成し、実装しない限り、1つのプライマリ展開（名前を変更しなければ「デフォルト展開」と呼ばれる）は、自動ですべてのドメインとサービスを自動包囲します。このプライマリ展開は、名前を変更してもメンバーがいなくても削除できません。

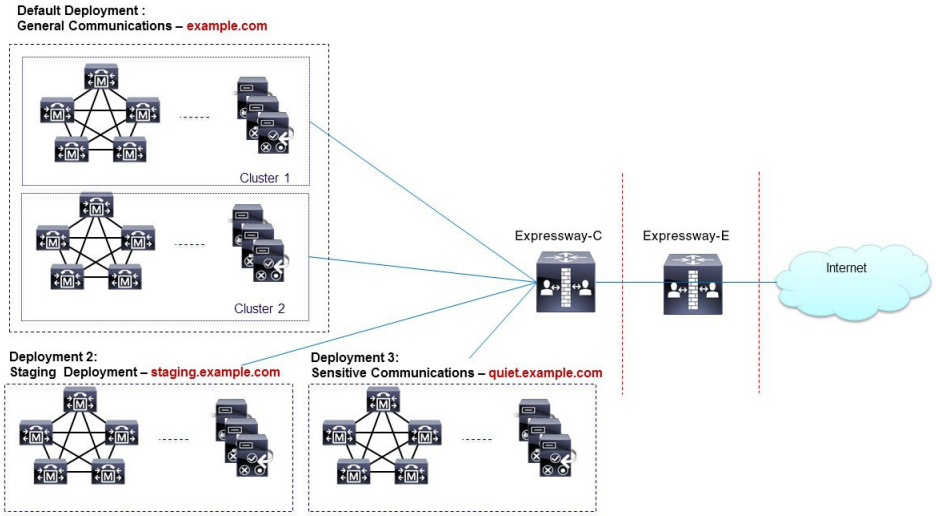
モバイルおよびリモートアクセスを介したサービスをパーティション化するには、必要な数の展開を作成します。それぞれに異なるドメインを関連付けたら、必要な Unified Communications リソースを各展開に関連付けます。

1 つのドメインを 1 つ以上の展開に関連付けることはできません。同様に、各 Unified Communications ノードには、1 つの展開のみ割り当てることができます。

例

2 つの Unified Communications インフラストラクチャを本運用 MRA 環境とステージング環境にそれぞれ実装するとします。この実装には、3 つ目のセットとして機密通信用の独立した環境も必要になる場合があります。

図 *1*: ネットワーク外からアクセスする *Unified Communications* サービスをパーティション化する複数展開



UC サービスの展開パーティションの割り当て

複数の内部 UC クラスタがあり、境界を作成して内部 UC サービスを分割する場合は、このオプションの手順を使用します。これが役立つ例の 1 つは、企業 UC サービス用のクラスタと 2 つ目のステージングクラスタがある場合です。

（注） 新しい展開を作成しない場合、すべての内部 UC アプリケーションは、単一の企業全体のデフォルト展開に属します。

ステップ 1 Expressway-C で、展開を作成します。

a) **[設定（構成）]** > **[Unified Communications]** > **[展開（Deployments）]** の順に選択し、**[新規（New）]** をクリックします。

b) 新しい展開を作成します。
c) 追加する展開ごとに繰り返します。

ステップ 2 展開に UC ドメインを割り当てます。

a) **[構成（Configuration）]** > **[ドメイン（Domains）]** の順に選択します。
b) 割り当てるドメインを選択します。
c) このドメインに割り当てる**展開**を選択します。
d) **[保存（Save）]** をクリックします。
e) この手順をくりかえし、追加のドメインに展開を割り当てます。

ステップ 3 UC サービスを展開に割り当てます。

a) **[構成（Configuration）]** > **[Unified Communications]**の順に選択し、関連する UC アプリケーションを選択します。
b) 割り当てるサーバーを選択します。
c) **[展開（Deployment）]** フィールドで、割り当てる展開を選択します。
d) [保存（Save）] をクリックします。
e) 各 UC クラスタの各ノードにこれを繰り返します。

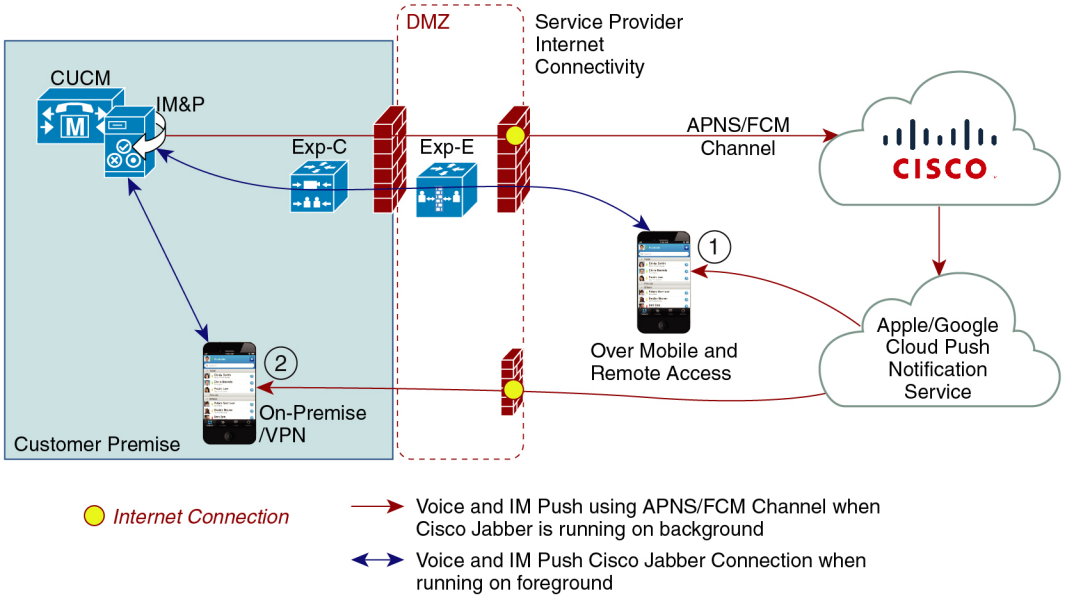
MRA 経由のプッシュ構成

MRA 展開に、iOS または Android デバイスで実行される Cisco Jabber または Webex クライアントが含まれている場合は、プッシュ構成を展開する必要があります。プッシュ構成がない場合、バックグラウンドモードに入ったクライアントにコールやメッセージを送信できない場合があります。

プッシュ構成の動作

クラスタでプッシュ構成が有効になっている場合、Cisco Unified Communications Manager と IM and Presence Service は、Apple または Google のいずれかのプッシュ構成サービスを使用してコールにプッシュ構成を、iOS または Android デバイスで実行する Cisco Jabber または Webex クライアントにメッセージを送信します。プッシュ構成を使用すると、システムがバックグラウンドモード（サスペンドモードとも呼ばれる）に入った後でも、クライアントと通信できます。プッシュ構成がない場合、バックグラウンドモードに入ったクライアントにコールやメッセージを送信できない場合があります。

起動時に、Android および iOS プラットフォームデバイスにインストールされているモバイルおよびリモートの Cisco Jabber または Cisco Webex クライアントは、Expressway-E を介して Cisco Unified Communications Manager および IM and Presence Service に登録されます。クライアントがフォアグラウンドモードのままである限り、新しいコールまたはメッセージを Expressway-E 経由でクライアントに送信できます。ただし、クライアントがバックグラウンドモードに移行すると、標準の通信チャネルは使用できなくなります。プッシュ構成は、該当するパートナークラウド（Apple または Google）を介してクライアントに到達するために大体チャネルを提供します。



プッシュ構成要件

Expressway-E が、Jabber iOS デバイス用にモバイルおよびリモートアクセス（MRA）をすでに提供している場合、プッシュ構成に対しては、Expressway での特定の構成は必要ありません。ただし、次の前提条件および推奨事項が適用されます。

- Expressway のプッシュ構成には、Apple クラウドの Cisco Jabber とプッシュ構成サーバー間でネットワークが必要です。

  インターネットに接続していないプライベートネットワークでは動作しません。

- Expressway は、すでに Jabber for iPhone/iPad に対してモバイルおよびリモートアクセスを提供しています。MRA は完全に構成されている必要があります（ドメイン、ゾーン、サーバ設定）。

- Unified CM 構成に応じて、プッシュ構成を Cisco コラボレーション クラウド に送信するためにフォワードプロキシが必要な場合があります。

- 自己記述トークン承認を使用することを推奨します。

- インスタントメッセージによるプッシュ構成には、Expressway-E の再起動が必要です。IM and Presence Service でプッシュ構成を有効化したら、Expressway-E を再起動する必要があります。再起動するまで、Expressway-E は、IM and Presence Service でプッシュ機能を認識できず、Jabber クライアントに PUSH メッセージを送信しません。

MRA のプッシュ構成の構成

MRA 経由でプッシュ構成を展開する場合は、次の要件があります。

- OAuth トークンの検証は、Expressway で構成する必要があります。
- Cisco Cloud サービスへの HTTPS 接続にフォワードプロキシ サーバーを使用するように Unified CM を構成する必要があります。

（注） Expressway の以前の組み込みフォワードプロキシは、X12.6.2 以降のバージョンの製品から削除されています。以前の Expressway バージョンでは、組み込みフォワードプロキシはサポートされていないため、使用しないでください。

詳細な手順については、『プッシュ構成導入ガイド』を参照してください。

Android デバイスでプッシュ構成を有効化

この機能は、 Expressway コマンド ライン インターフェイスを介して有効化されます。

MRA を介した Android 用の PUSH 対応 CLI コマンド： **xConfiguration XCP Config FcmService: On**

Note

- この操作は、Android ユーザーにサービスを提供する IM and Presence Service のすべてのノードでサポート対象のリリースを実行している場合に**のみ**実行します。
- この機能を使用して、Expressway-E のみをオンにする必要があります。
- このコマンドを使用すると、MRA を介して現在サインインしているユーザの IM and Presence サービスが中断されます。このため、これらのユーザは再度サインインする必要があります。

このテーブルは、Androidプッシュ構成用のExpressway CLI 対応/非対応コマンドを示しています。管理者は、CLI コマンドをオンにするかオフにするかを決定できます。

Table 1: ソリューションマトリックス

混合バージョンの IM&P クラスタ	Expressway X12.7 の FCM フラフの想定ステータス	コメント
12.5(1) SU2以降をの任意の 11.5(1) SU	オフ	Android プッシュ（FCM）はサポートされていません
11.5(1) SU8 以降または 12.5(1) SU2 以降と 12.5(1) SU3	オフ	Android プッシュ（FCM）はサポートされていません

混合バージョンの IM&P クラスタ	Expressway X12.7 の FCM フラフの想定ステータス	コメント
11.5(1) SU8 以降または 12.5(1) SU2 以降と 12.5(1) SU4 以降	オフ	12.5(1) SU4 以降のバージョンでサポートされている Android プッシュ（FCM）
11.5(1) SU9 以降または 12.5(1) SU4 以降と 12.5(1) SU3	ON	すべての 12.5(1) バージョンでサポートされている Android プッシュ（FCM）
11.5(1) SU9 以降と 12.5(1) SU4 以降	フラグは不要です （Expressway X12.7新しい検出メカニズムに完全に依存しています）	12.5(1) SU4 以降のバージョンでサポートされている Android プッシュ（FCM）

モバイルアプリケーション管理クライアントを使用したプッシュ通知：MRA 展開

この機能は、Mobile and Remote Access を使用して Expressway を展開する場合に該当します。

この機能を使用すると、Jabber Intune や Jabber BlackBerry などのモバイル アプリケーション管理（MAM）クライアントが、Mobile and Remote Access を介したプッシュ通知のサポート対象になります。その結果、Jabber Intune クライアントや Jabber BlackBerry クライアントを実行しているすべてのデバイスでプッシュ通知サービスを利用できます。

詳細については、『プッシュ通知導入ガイド』>「プッシュ通知（オンプレミス展開）」を参照してください。

ファストパス登録

ファストパス登録の構成

（注） ファストパス登録を有効にするために事前ルーティングルートヘッダー（PRRH）を有効にした後、Expressway-E を再起動します。

ファストパス登録が有効な場合、Expressway は、最初のルーティング計算をキャッシュしてから、事前にルーティングしたルートヘッダーを使用して、キャッシュされたルーティング結果を使用して後続のパケットをルートします。この機能は、サーバーのワークロードを削減し、キャパシティを増加させます。

Expressway-Eで、次のコマンドを使用して、ダイジェストキャッシュ間隔とダイジェストキャッシュライフタイムの両方を 7200 に設定します。

- `xConfiguration Authentication Remote Digest Cache ExpireCheckInterval：「7200」`
- `xConfiguration Authentication Remote Digest Cache Lifetime：「7200」`

SIP パスヘッダーの有効化

Expressway-C のデフォルト設定は、SIP REGISTER メッセージの Contact ヘッダーをリライトします。SIP Path ヘッダーを有効化すると、Expressway-C は Path ヘッダーにアドレスを追加しますが、Contactヘッダーには追加しません。この設定は、次のような一部の機能がMRAを介して動作するために必要です。

- 共有回線および複数回線
- BiB 通話録音
- サイレント モニタリング
- キー拡張モジュール

（注） 11.5(1)SU4 の最小の Unified CM リリースを展開することをお勧めします。詳細については、CSCvd84831 を参照してください。

ステップ 1 Expressway-C で、SIP Path ヘッダーをオンにする

a) Expressway-Cで、**[構成（Configuration）] > [Unified Communications] > [構成（Configuration）]**の順に選択します。
b) **[SIP Pathヘッダー（SIP Path headers）]** を **オン**にします。
c) [保存（Save）] をクリックします。

ステップ 2 設定を保存したら、Unified CM サーバーを更新します。

a) **[構成（Configuration）] > [Unified Communications] > [Unified CMサーバー（Unified CM servers）]** の順に選択します。
b) **[サーバーの更新（Refresh server）]** をクリックします。

Unified CM と Expressway-C 間の SIP トランク

モバイルおよびリモートアクセスの Expressway 展開では、Unified CM と Expressway-C 間の SIP トランク接続は必要ありません。 Expressway-C と検出された Unified CM ノードの間に自動生成されたネイバーゾーンは SIP トランクではないことに注意してください。

ただし、必要に応じて SIP トランクを構成することもできます。（たとえば、B2B 発信者または Expressway に登録されたエンドポイントを有効化して、Unified CM に登録されたエンドポイントにコールするなどが挙げられます。）

SIP トランクが構成されている場合、Unified CMUnified CM への SIP 回線登録に使用されるポートとは別のリスニング ポートを Unified CM で使用する必要があります。競合が起きると、Expressway-C でアラームが出ます。

SIP トランクで使用するポートは、Unified CM と Expressway の両方で構成されます。

SIP トランクの構成詳細については、『Cisco Expressway SIP トランクから Unified CM 導入ガイド』を参照してください。

SIP トランクに OAuth ベースの認証を設定する方法については、「UC アプリケーションで OAuth を構成する」を参照してください。

トランク接続用の SIP ポートの構成

Expressway と Cisco Unified Communications Manager の間に SIP トランクを構成した場合は、この手順を使用して、トランクが使用するポート設定を構成します。

ステップ 1 Unified CM の回線登録リスニングポートの設定

a) Cisco Unified CM Administration で、**[システム（System）]** > **[Cisco Unified CM]** の順に選択します。
b) **[SIP 電話ポート（SIP Phone Port）]** を **5060** に設定します。
c) **[SIP 電話のセキュア ポート（SIP Phone Secure Port）]** を **5061** に設定します。
d) [保存（Save）] をクリックします。

ステップ 2 Unified CM のトランク リスニング ポートの設定

a) Cisco Unified CM Administration で、**[システム（System）]** > **[セキュリティ（Security）]** > **[SIPトランクのセキュリティプロファイル（SIP Trunk Security Profile）]** の順に選択します。
b) **[検索（Find）]** をクリックして、SIP トランクに使用しているプロファイルを選択します。
c) **着信ポート**を回線ポートとは異なるように構成します。
d) **[保存（Save）]** をクリックして、**[構成を適用（Apply Config）]** をクリックします。

ステップ 3 Expressway で SIP トランクリスニング ポートを設定します。

a) Expressway-C で、**[構成（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** の順に選択します。
b) SIP トランクに使用する Unified CM ネイバーゾーンを選択します。

c) **SIP ポート**を、SIP トランク セキュリティ プロファイルで構成された**着信ポート**と同じ値に設定します。
d) [保存（Save）] をクリックします。

MRA 経由の BiB レコード

Expressway は、MRA 経由の組み込みブリッジ（BiB）録音をサポートしています。この機能は、欧州連合の Markets in Financial Instruments Directive（MiFID II）における電話録音の要件を遵守するのに役立ちます。

提供内容の概要

- BiB を使用して、オフプレミスで作業しているユーザが発信または受信したコールの音声部分を録音できます。
- BiB は Expressway で常に有効になっています。
- BiB は Cisco Unified Communications Manager で設定できます。BiB が有効になっている場合、Unified CM は、エンドポイント間での発着コールをメディア録音サーバにフォークします。

帯域幅とキャパシティの要件

この機能を使用する場合は、帯域幅とコールキャパシティに大きな影響を与えることに注意してください。

- 追加のネットワーク帯域幅をプロビジョニングする必要があります。詳細については、「シスコ コラボレーション システム 12.x ソリューション リファレンス ネットワーク デザイン（SRND）」の「監視および録音用キャパシティプラン」項を参照してください。MRA エンドポイントに対して BiB を有効にするには、通常 2 倍の帯域幅が必要です。これは、コールの発信側と着信側の両方が録音されると仮定すると、BiB 対応の各コールが通常の 2 倍の帯域幅を消費するためです。
- MRA エンドポイントで BiB を有効にすると、Expressway ノードの全体的なコール キャパシティが元のキャパシティの約 3 分の 1 に減少します。これは、録音されている各通話に、それに関連付けられた 2 つの追加の SIP ダイアログがあるためです（したがって、本質的に 3 つの通話に相当します）。

設定要件

MRA を介して BiB Recording を展開するには、次のように構成します。

- BiB 録音を Cisco Unified Communications Manager で構成します。手順の詳細については、「*Cisco Unified Communications Manager* 向け機能構成ガイド」の「通話録音」章を参照してください。

- SIP パスヘッダーは、Expressway で有効にします。詳細については、SIP パスヘッダーの有効化 （7 ページ）を参照してください。

さらに、次の要件も満たす必要があります。

- 互換性のあるクライアントが必要です
  - Windows 版 Cisco Jabber 11.9
  - Mac 版 Cisco Jabber 11.9
  - iPhone および iPad 版 Cisco Jabber 11.9
  - Android 版 Cisco Jabber 11.9
  - MRA 対応の Cisco IP Phone 7800 シリーズ、Cisco IP Conference Phone 7832 または Cisco IP Phone 7800 シリーズ デバイス（これらすべての電話が MRA 対応であるとは限りません）
  - 現在 MRA に対応している電話に関しては、このガイドの「MRA インフラストラクチャ要件」項を参照するか、シスコ担当者にお問い合わせください。
- レジストラ/呼制御エージェント：Cisco Unified Communications Manager 11.5(1)SU3 BiB は、Expressway 登録エンドポイントではサポートされていません。
- エッジ トラバーサル：Expressway X8.11.1 以降
- レコーディング サーバ：このドキュメントの範囲外です。（Cisco Unified Communications Manager における録音の設定方法の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』を参照してください。）

HTTP 許可リスト

HTTP 許可リストは、HTTP サービスのアクセスリストの一種です。Expressway-C は、インバウンドルールとアウトバウンドルールの両方を自動追加します。たとえば、Expressway は、MRA 構成中に検出された Unified Communications ノードに外部クライアントがアクセスできるようにするインバウンドルールを自動追加します。これらには、Unified CM ノード（CallManager および TFTP サービスを実行する）、IM and Presence Service ノード、および Cisco Unity Connection ノードが含まれます。

ただし、場合によっては、特定のタイプのアクセスを許可するためにインバウンドルールを編集する必要があります。アウトバウンドルールは編集できません。

- インバウンドルールを表示するには、**[構成（Configuration）] > [Unified Communications] > [HTTP許可リスト（HTTP allow list）] > [自動インバウンドルール（Automatic inbound rules）]**の順に選択します。
- アウトバウンドルールを表示するには、**[構成（Configuration）] > [Unified Communications] > [HTTP許可リスト（HTTP allow list）] > [自動アウトバウンドルール（Automatic outbound rules）]**の順に選択します。

HTTP 許可リストの編集

リモートクライアントが企業内の他の Web サービスにアクセスする必要がある場合は、独自のインバウンドルールをHTTP許可リストに追加できます。たとえば、次のサービスでは許可リストの構成が必要になる場合があります。

- Jabber アップデート サーバ
- Cisco Extension Mobility
- ディレクトリ フォト ホスト
- マネージド ファイル転送
- Problem Report Tool サーバー
- ビジュアル ボイスメール

<link to Appendix and other places for more info>

HTTP 許可リストにアウトバウンドルールを追加することはできません。また、リストに自動追加されたルールを編集または削除することはできません。

（注） [マネージドファイル転送（Managed File Transfer）] 機能が Expressway 全体で機能するようにするには、手動または自動で追加されたかどうかにかかわらず、すべての Unified CM IM and Presence Service ノードが許可リストに表示されていることを確認してください。

自動インバウンドルール

Expressway は、Unified Communications ノードを検出または更新すると、HTTP 許可リストを自動編集します。このページには、検出されたノードと、それらのノードに適用されるルールが表示されます。

最初のリストは検出されたノードであり、この Expressway-C で現在認識されているすべてのノードが含まれています。各ノードのリストには、ノードのアドレス、タイプ、および発行元のアドレスが含まれています。

2 番目のリストは、さまざまなタイプの Unified Communications ノードへのクライアントアクセスを制御するために追加されたルールです。MRA 構成のノードのタイプごとに、このリストに1つ以上のルールが表示されます。編集可能なルールと同じ形式で表示されますが、これらのルールを変更することはできません。

表 *2:* 自動追加された許可リストルールのプロパティ

列	説明
タイプ	このルールは、リストされているタイプのすべてのノードに影響します。 • Unified CM サーバー： Cisco Unified Communications Manager ノード • IM and Presence Service ノード： Cisco Unified Communications Manager IM and Presence Service ノード • Unity Connection サーバー：Cisco Unity Connection ノード • TFTP：TFTP ノード
プロトコル	クライアントがこれらのタイプのノードと通信することをルールが許可するプロトコル。
ポート	クライアントがこれらのタイプのノードと通信することをルールが許可するポート。
一致タイプ	*Exact* または *Prefix*。このルールを使用してクライアントがアクセスするサービスの性質に応じる。
パス	このルールを使用したクライアントがアクセスするリソースへのパス。ルールで *Prefix* 一致が許可されている場合、これは存在しないか、実際のリソースの部分一致のみである可能性があります。
仕組み	このルールが許可する HTTP メソッド（**GET** など）。

HTTP 許可リストの編集

ステップ 1 **[構成（Configuration）] > [Unified Communications] > [HTTP許可リスト（HTTP allow list）] > [編集可能なインバウンドルール（Editable inbound rules）]** の順に選択し、HTTP 許可リストルールを表示、作成、修正、削除します。

このページには 2 つの領域があります。1 つはデフォルトの HTTP メソッドを制御するためのもので、もう 1 つは編集可能なルールを表示するためのものです。

ステップ 2 （任意） チェックボックスを使用してデフォルトの HTTP メソッドのセットを変更し、**[保存（Save）]** をクリックします。

個々のルールを編集しているときに、デフォルトをオーバーライドできます。可能な限り安全にしたい場合は、デフォルトセットからすべてのメソッドをクリアし、ルールごとにメソッドを指定します。

デフォルトの方法を変更すると、以前にデフォルトの方法で作成したすべてのルールで新しいデフォルトが使用されます。

ステップ 3 [推奨]左側の列のチェックボックスをオンにし、**[削除（Delete）]**をクリックすると不要なルールを削除できます。

ステップ 4 **[新規（New）]** をクリックし、ルールを作成します。

ステップ 5 要件に合わせてルールを構成します。

ここでは、各フィールドに対するアドバイスをいくつか紹介します。

表 *3*：手動追加した許可リストルールのプロパティ

列	説明
Description	目的を認識しやすくするために、このルールの分かりやすい説明を入力します。
Url	MRA クライアントがアクセスできる URL を指定します。たとえば、**`http://www.example.com:8080/resource/path`** へのアクセスを許可するには、この URL をそのまま入力します。 • クライアントがホストにアクセスするために使用しているプロトコルは、http:// または https:// である必要があります。 • デフォルト以外のポートを使用する場合は、ポートを指定します（例：8080）。 （デフォルトポートは、80（http）と 443（https）です） • ルールの範囲を制限する（より安全な）パスを指定します（例：/resource/path）。 このルールで、**[プレフィックスの一致（Prefix match）]** を選択した場合、部分的なパスを使用するか、パスを省略できます。対象のリソースが不正な URL に対してレジリエンシがない場合、これはセキュリティリスクになる可能性があることに注意してください。
許可された方式	**[デフォルトを使用（Use defaults）]** または **[方法を選択（Choose methods）]** を選択します。 このルールに特定の HTTP メソッドを選択すると、すべてのルールに対して選択したデフォルトがオーバーライドされます。
一致タイプ	**[完全一致（Exact match）]** または **[プレフィックス一致（Prefix match）]** を選択します。 ここでの判断は、環境によって異なります。[完全一致（Exact match）] を使用する方が安全ですが、より多くのルールが必要になる場合があります。[プレフィックス一致（Prefix match）] を使用する方が便利ですが、意図せずにサーバーリソースを公開するリスクがあります。
導入	MRA 環境で複数の展開を使用している場合は、新しいルールを使用する展開も選択する必要があります。複数の展開がない限り、このフィールドは表示されません。

ステップ 6 **[エントリの作成（Create Entry）]** をクリックしてルールを保存し、編集可能な許可リストに戻ります。

ステップ 7 （任意）ルールを変更するには、**[表示/編集（View/Edit）]** をクリックします。

ルールを HTTP 許可リストにアップロード

（注） アウトバウンドルールをアップロードすることはできません。

ステップ 1 **[構成（Configuration）]** > **[Unified Communications]** > **[HTTP許可リスト（HTTP allow list）]** > **[ルールをアップロード（Upload rules）]** の順に選択します。

ステップ 2 ルール定義を含む CSV ファイルを参照して選択します。

許可リストによるファイル参照の決定を参照してください。

ステップ 3 [アップロード（Upload）] をクリックします。

Expressway は成功メッセージで応答し、**[編集可能なインバウンドルール（Editable inbound rules）]** ページを表示します。

MRA 経由の Dial via Office-Reverse

モバイルワーカーは、オフィスで電話をかけるときと同じ高品質、セキュリティ、信頼性を必要としています。Dial via Office-Reverse（DVO-R）機能を有効にして、デュアルモードモバイル デバイスで Cisco Jabber を使用している場合は、そのことを保証できます。DVO-R は、企業を介して Cisco Jabber call を自動的にルーティングします。

DVO-R は、コールシグナリングと音声メディアを別々に処理します。Expressway でのモバイルおよびリモートアクセスのシグナリングを含むコールシグナリングは、クライアントと Cisco Unified Communications Manager 間の IP 接続を通過します。音声メディアは、企業の公衆電話交換網（PSTN）（PSTN）ゲートウェイのセルラーインターフェイスとヘアピンを通過します。オーディオをセルラーインターフェイスに移動すると、IP 接続が失われた場合でも、高品質な通話とオーディオは安全に維持されます。

DVO-R を構成して、ユーザーが通話発信したときに、Cisco Unified Communications Manager からの折り返し通話が次のいずれかに送信されるようにすることができます。

- ユーザーのモバイル ID（携帯電話番号）。
- ユーザーの代替番号（ホテルの部屋など）。

DVO-R over MRA のコールフローの例

次のコールフローは、モバイル ID または代替番号のいずれかに折り返し通話を送信する場合の、MRA 通話経由の Dial via Office Reverse について説明します。コールフローの図については、後続の画像を参照してください。

1. 番号をダイヤルすると、信号が IP パス（WLAN またはモバイル ネットワーク）を介して Cisco Unified Communications Manager に送信されます。
2. Cisco Unified Communications Manager は、自分の携帯電話番号または設定した代替番号に電話をかけます。
3. 応答すると、Cisco Unified Communications Manager はダイヤルした番号に通話を転送し、呼び出し音が鳴ります。
4. その人が応答すると、進行中の通話は企業の PSTN ゲートウェイでヘアピンされ、次の処理が行われます。
   - モバイル ID を使用すると、通話は企業ゲートウェイに固定されます。通話は携帯電話とデスクフォンでアクティブであるため、この 2 つを切り替えることができます。
   - 代替番号を使用すると、進行中の通話は固定されず、デスクフォンには出られません。

図 *2*：モバイル *ID* を使用した *MRA* 経由の *DVO-R*

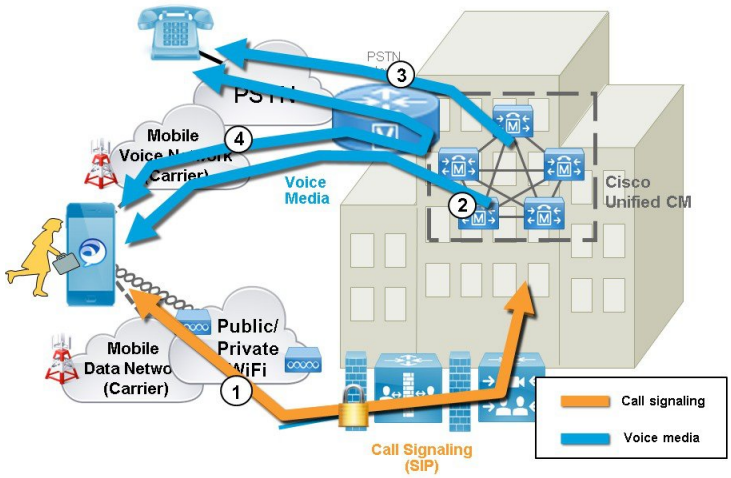
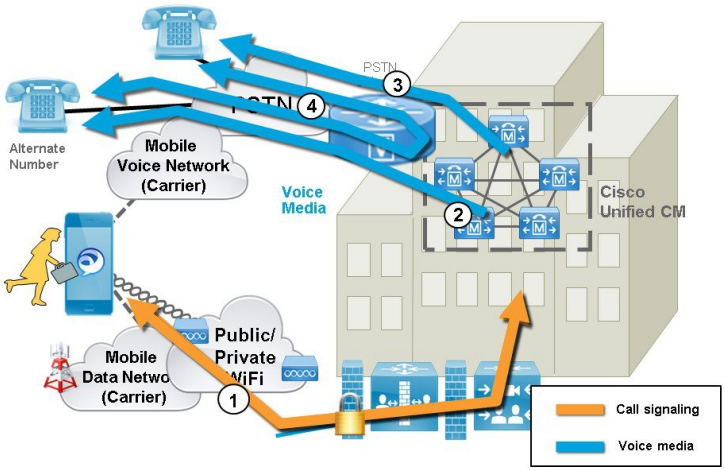


図 *3:* 代替番号を使用した *MRA* 経由の *DVO-R*



DVO の要件

この機能は、関連システムの次のバージョンで必要です。

- Cisco Unified Communications Manager 11.0(1) 以降
- Cisco Jabber 11.1 以降

補足事項

- PSTN ゲートウェイと Cisco Unified Communications Manager 間にアウトオブバンド DTMF リレーがある場合、アンカーされたコールで Dual Tone Multi Frequency（DTMF）ベースの通話中機能（例：保留は *81）を使用できます代替番号を使用している場合は、通話中機能を利用できません。
- Cisco Unified Communications Manager からのコールバックレッグがボイスメールにルーティングされるのを防ぎ、ダイヤルしている相手にボイスメールコールが届かないようにするには、DVO-R ボイスメール ポリシーを [ユーザ制御ー（user controlled）] に設定することをお勧めします。これにより、通話を続行する前に、キーパッドのいずれかのキーを押して DTMF トーンを生成する必要があります。

MRA 経由の Dial via Office-Reverse の構成

DVO-R を MRA 上で機能させるための Expressway 構成要件はありません。ただし、Unified CM ノードと Cisco Jabber クライアントで必要な構成があります。ハイレベルでの構成は次のとおりです。

ステップ 1 DVO-R をサポートするように Cisco Unified Communications Manager を設定します。
ステップ 2 各デバイスに DVO-R を設定します。
ステップ 3 ユーザー制御によるボイスメールを無効に設定します。

ステップ 4 リモート接続先の追加（オプション）。

ステップ 5 Cisco Jabber クライアント設定を構成します。

（注） UC アプリケーションとクライアントを構成し、モバイルおよびリモートアクセスで Dial via Office-Reverse を機能させる方法について説明する詳細な構成例は、https://www.cisco.com/c/en/us/support/docs/unified-communications/expressway/200198-Configuring-Dial-via-Office-Reverse-to-W.html の 「モバイルおよびリモートアクセスで *Dial via Office-Reverse* を機能するよう構成する」を参照してください。

マルチクラスタのベストプラクティス

このセクションでは、マルチクラスタ MRA 展開を構成するためのヒントとベストプラクティスについて概説します。次に、マルチクラスタ MRA 展開を構成する際に留意すべきいくつかのベストプラクティスを示します。

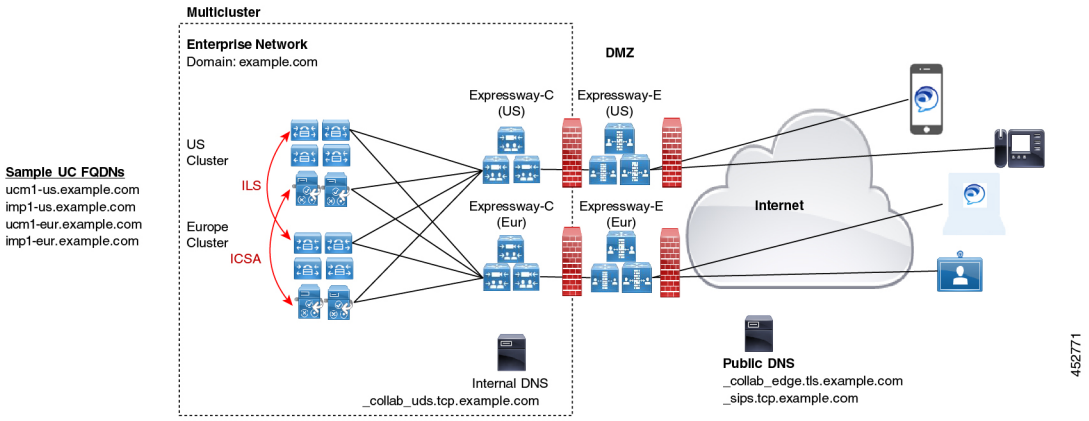
- すべての Expressway-C クラスタを、すべての UC クラスタに接続する必要があります。そうしないと、Expressway-C はすべての UC クラスタに要求をプロキシできません。各 Expressway-C クラスタのプライマリピアで、Expressway-C が到達する必要がある各 UC クラスタのパブリッシャ ノードを追加してから、サーバーを更新します。これにより、さまざまな UC クラスタからの残りのサブスクライバノードが Expressway-C に入力されます。
- 一部のクラスタが SIP ドメインを共有している場合：各ユーザーが特定のクラスタに割り当てられるように、各ユーザーの **[ホームクラスタ（Home Cluster）]** 設定を有効にする必要があります。この設定は、Cisco Unified Communications Manager の **[エンドユーザー構成（End User Configuration）]** ウィンドウに表示されます。
- 同じドメイン内に複数の Unified CM クラスタがある場合、特に大規模なクラスタ間ネットワークでは、クラスタ間検索サービス (ILS) が推奨されます。初期設定後、ILS は ILS ネットワーク全体で自動クラスタ検出とダイヤルプラン レプリケーションを提供します。ただし、クラスタ検出は手動で構成できるため、ILS は必須ではないことに注意してください。ILS の構成方法については、『*Cisco Unified Communications Manager* 向け システム構成ガイド』を参照してください。
- 同じドメイン内に複数の IM and Presence Service クラスタがある場合は、同じドメインにある IM and Presence クラスタの Intercluster Sync Agent（ICSA）を使用してクラスタ間ピアリングを構成する必要があります。クラスタ間ピアリングの構成方法については、『*IM and Presence Service* 向け構成およびアドミニストレーション ガイド』を参照してください。
- 複数の Edge クラスタがある場合は、それらの間で負荷分散を構成します
  - これらのエッジが同じデータセンターにある場合は、負荷分散にドメインネームシステム（DNS）SRV を使用できます。

- エッジが地理的境界（異なる都市または大陸）にまたがって分割されている場合は、GeoDNS を使用できます。GeoDNS SRV レコードを使用してリクエストを適切なエッジサーバーにルーティングする方法の例については、以下を参照してください。

マルチクラスタの GeoDNS の例

GeoDNS over MRA は、クライアントが MRA に使用される Expressway から比較的離れている場合に、最も近い Expressway を提供するという特定の目的でサポートされます。これにより、待ち時間とネットワーク遅延を最小限に抑えることができます。

次の例は、複数の Unified CM クラスタに接続する 2 つの Expressway-C クラスタを使用したマルチクラスタ展開を示しています。この例では、単一のドメインを使用していますが、地理的に離れた 2 つの Expressway クラスタを使用しているため、2 つのエンタープライズエッジが提供されます。DNS プロバイダーによっては、GeoDNS を SRV または CNAME レコードに適用できます（SRV が使用可能な場合は優先されます）。以下は、2 つの Edge ドメイン（1 つはヨーロッパにあり、もう 1 つは米国にある Edge）がある場合に、GeoDNS を使用する方法の 2 つの例です。



ドメインネームシステム（DNS）プロバイダーがサポートしている場合、推奨される SRV アプローチは、ユーザーの場所（たとえば、米国またはヨーロッパ）に基づく優先度設定での SRV レコード作成です。SRV は、ユーザーの場所と、各エッジサーバーに割り当てられている優先度設定を使用して、要求の送信先のサーバーを決定します。その要求が失敗した場合、他のサーバーはバックアップオプションを提供します。

表 *4 : SRV* レコードの *GeoDNS*（推奨アプローチ）

SRV レコード	ユーザの場所	ルート先（優先）
_collab-edge.tls.example.com _sips_tcp.example.com	US	• us-expc.example.com (10) • eur-expc.example.com (20)
	ヨーロッパ	• eur-expc.example.com (10) • us-expc.example.com (20)

以下は、2つのCNAMEエイリアス（メインエイリアスと優先度の低いバックアップCNAME）にルーティングする GeoDNS SRV 構成レコードの例です。各 CNAME レコードは、ユーザーの場所に基づいて異なるサーバーに通話をルーティングします。メインCNAMEに障害がある場合、バックアップ CNAME は通話を別のリージョンのサーバーに送信します（NA ユーザーはヨーロッパベースの Expressway にルーティングされます）。

表 *5 : CNAME* 経由の *GeoDNS* ルーティング

SRV レコード	CNAME へのルーティング（優先）	ユーザの場所	ルート先
_collab-edge.tls.example.com _sips_tcp.example.com	alias1.example.com (10)	US	us-expc.example.com
		ヨーロッパ	eur-expc.example.com
	backup-alias1.example.com (20)	US	eur-expc.example.com
		ヨーロッパ	us-expc.example.com

（注） SRV アプローチでは、SRV の重み設定をすべてのレコードで同じままにします。

（注） 発信者のロケーションに基づいて通話をルーティングできるように、UnifiedCM で地理ベースのコーリングサーチスペースとパーティションを設定する必要がある場合もあります。たとえば、地理ベースのコーリングサーチスペース（特定の都市のCSS）を作成し、その都市にあるすべての電話をその CSS 内に配置できます（1 つの CSS は「New_York_CSS」と呼ばれ、別の CSS は「Chicago_CSS」と呼ばれる場合があります)」）

詳細については、https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Collaboration/enterprise/12x/120/collbcvd/edge.html#pgfId-1081382 の「シスコ コラボレーション *12.x* 企業オンプレミス展開向け優先アーキテクチャ」に記載されている「コラボレーション エッジ ソリューションのスケーリング」を参照してください。

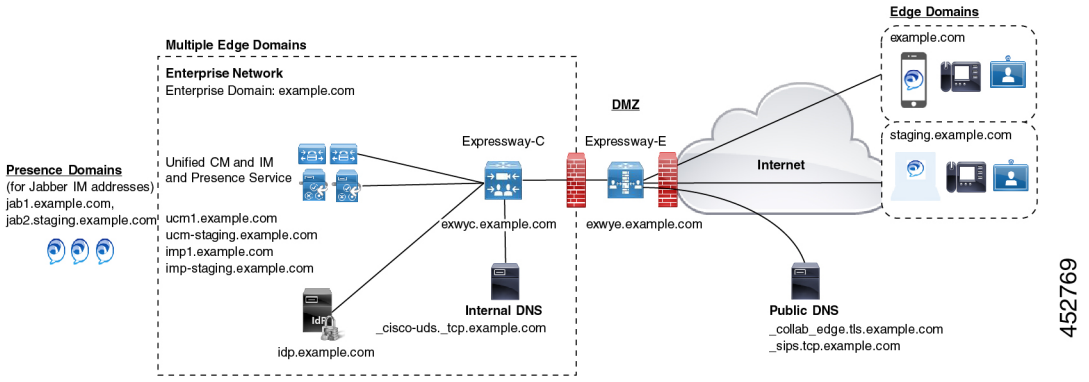
マルチドメインのベストプラクティス

このセクションでは、複数のドメインで MRA を展開するお客様向けに、ドメイン関連の情報と構成プロセスの概要を説明します。モバイルおよびリモートアクセスの理想的なシナリオは、すべてのコラボレーションアプリケーションとエンドポイントに対して単一ドメインを割り当てることですが、これがすべての場合に可能であるとは限りません。ネットワークによっては、マルチドメイン設定の複雑さのレベルが異なる場合があるため、ドメイン設定を使用できるさまざまなコンテキストを理解することが重要です。

複数エッジドメイン

次の図は、内部 UC ドメインが外部ドメインと異なる基本的なマルチドメインシナリオを示しています。

図 *4:* 複数エッジドメイン

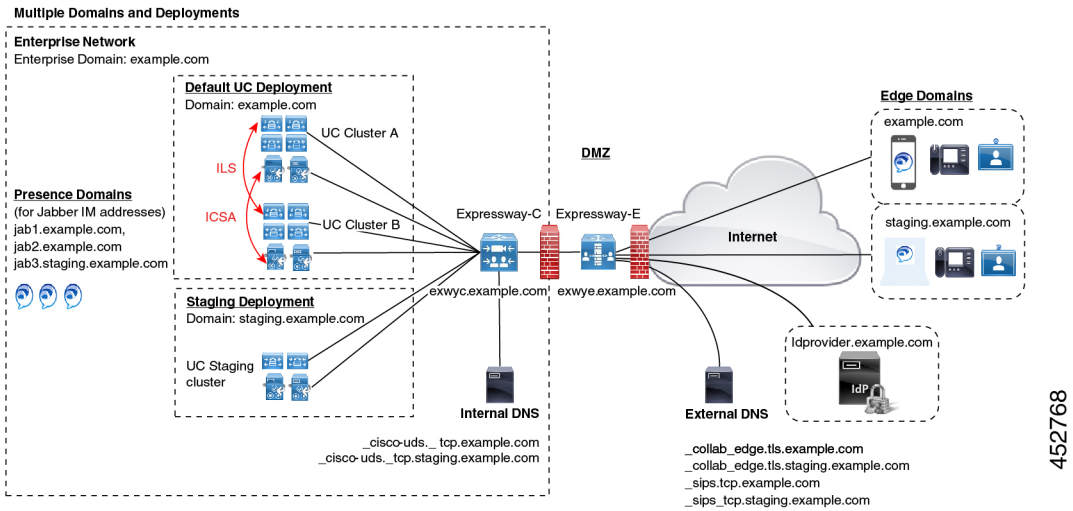


（注） MRA エンドポイントは、Expressway-E に到達できるように、外部パブリック ドメインネームシステム（DNS）サーバーに接続できる必要があります。

個別のデプロイメントを持つ複数のドメイン

次の例は、内部 UC 環境が 2 つの展開（デフォルトの UC 展開）に分割されている、より複雑なマルチドメインシナリオを示しています。これには、Expressway と 2 番目のステージング展開の両方を含む、メインの UC アプリケーションが含まれます。2 つの展開は、異なるドメインにあります。デフォルトの展開には、ILS と ICSA を使用して内部クラスタ間でデータを同期する複数の UC クラスタがあります。この例では、別の外部 IdP ドメインにあるクラウドベースの ID プロバイダーも使用しています。

図 *5:* 個別のデプロイメントを持つ複数のドメイン



ドメイン用語一覧

次の表は、MRA 展開内でドメイン用語を使用できるさまざまなコンテキストと、それらを Expressway で設定する方法を概説しています。展開によっては、これらすべてのコンテキストに同じドメインが適用される場合があります。

表 *6:* ドメイン用語一覧

用語	説明
エッジ ドメイン	この用語は、リモート MRA エンドポイントがオンプレミスの UC ネットワークに接続するリモートドメインを指します。これは、**[構成（Configuration）] > [ドメイン（Domain）]**メニューの Expressway-C で構成し、UC トラバーサルゾーンを経由して Expressway-E に通信されます。
Expressway サーバードメイン	Expressway-C と Expressway-E の場合、ドメインは各サーバーの FQDN アドレスの一部であり、それぞれのサーバーの **[システム（System）] > [ドメインネームシステム（DNS）（DNS）]** でプロビジョニングされます。各サーバーは、単一のドメインのみをサポートします。
内部 UC ドメイン	これは、Cisco Unified Communications Manager や IM and Presence Service などの内部 UC アプリケーションのドメインです。これらのアプリケーションは、Expressway と同じドメインにある場合もあれば、別のドメインにある場合もあります。 （注） 内部 UC アプリケーションが Expressway とは異なるドメインにある場合は、UC サーバーアドレスのサーバーアドレスとして FQDN または IP アドレスを使用する必要があります。FQDN が優先されます。

用語	説明
プレゼンスドメイン	プレゼンスドメインは IM and Presence Service で設定され、クライアントの IM アドレスで使用される場合があります（たとえば、user@domain）。 （注） MRA クライアントの場合、プレゼンスドメインがエッジドメインと同じでない場合は、プレゼンスドメインを Expressway-C のドメインリストに追加します。 （注） MRA を介した複数のプレゼンスドメインは、IM and Presence Service、リリース 10.0(1) 以降を備えた Expressway X12.6.3 でサポートされます。ただし、1 回の展開内で 75 ドメインを超えないようにすることをお勧めします。
MRA アクティベーションドメイン	MRA エンドポイントのアクティベーションコード導入準備を使用している場合、MRA アクティベーションドメインは、クラウドの導入準備プロセス中に Unified CM で設定され、最初のデバイスアクティベーションのためにそのクラスタの MRA エンドポイントが接続する必要があるドメインを表します。各クラスタは、単一の MRA アクティベーションドメインのみを持つことができます。
MRA サービスドメイン	MRA エンドポイントのアクティベーションコード導入準備を使用している場合、MRA サービスドメインは Unified CM で設定され、エンドポイントが通常の MRA 使用のために接続するリモートエッジドメインを表します。複数の Expressway クラスタがある場合、MRA サービスドメインでは、通常の MRA 操作に使用する Expressway クラスタを指定できます。 MRA デバイスが MRA アクティベーションドメイン内でアクティブ化されたら、デバイスは、割り当てられた MRA サービスドメインへのリダイレクトを含む構成ファイルをダウンロードします。次に、デバイスはそのドメインの `_collab_edge` SRV を検索し、ドメインに割り当てられている Expressway クラスタを介して登録を試行します。 MRA サービスドメインは、クラスタ、デバイスプール、または個々のデバイスレベルでエンドポイントに適用できます。 （注） MRA アクティベーションドメインは、Unified CM クラスタで使用可能な MRA サービスドメインのリストに自動追加されます。

マルチドメイン構成の概要

次の表は、マルチドメイン MRA シナリオのドメイン固有タスクの構成概要を示しています。

（注） この概要は、基本的な MRA 展開を設定するための主要な構成フローを置き換えるものではありません。主要な構成フローに従うことで、複数のドメインで MRA をサポートするようにシステムを構成できます。ただし、複雑なマルチドメインシナリオの場合、この概要は、ドメイン設定が正しいことを確認するために使用するドメイン固有タスクの便利なチェックリストとして使用できます。

表 *7: MRA* マルチドメイン構成の概要

手順	タスク
ステップ 1	Expressway サーバーのホスト名とドメイン名を構成します。 Expressway サーバーアドレスの設定を参照してください。
ステップ 2	Expressway-C で、Unified CM にルートする MRA 登録、呼制御、プロビジョニング、メッセージングおよびプレゼンスサービスに対してドメインを追加します。次も含まれます。 • 内部 UC ドメイン • エッジドメイン（内部ドメインと異なる場合） • プレゼンスドメイン（他のドメインと異なる場合） ドメインの追加を参照してください。
ステップ 3	(オプション)。展開を内部 UC アプリケーションに割り当てます。このオプション設定により、内部 UC サービスをパーティション化できます。たとえば、この構成を使用して、メインの本運用クラスタを別のステージングクラスタから切り離すことができます。 UC サービスの展開パーティションの割り当て （2 ページ）を参照してください。

手順	タスク
ステップ4	内部 DNS エントリの構成方法 **1.** `_cisco-uds._tcp.<domain>` SRV レコードを各 Unified CM ドメインに構成します。 **2.** Unified CM および IM and Presence ノードに対して正引きおよび reverse ルックアップを作成します。 **3.** Expressway-C を Expressway-E に向ける A および PTR レコードを設定します。 （注） X12.6 の時点で、MRA エンドポイントが正しい UC クラスタに到達できるようにするために、`_cisco_uds.tcp.example.com` 内部 SRV レコードは必須ではなくなりました。ただし、オンプレミスの Cisco Jabber および Webex クライアントを展開している場合は、この SRV レコードが引き続き必要であることに注意してください。 ローカルドメインネームシステム（DNS）（内部ドメイン）を参照してください。
ステップ5	パブリック ドメインネームシステム（DNS） の構成方法 **1.** Expressway-E で、エッジドメインに対して `_collab-edge._tls.<domain>` および `_sips_tcp.<domain>` ドメインネームシステム（DNS）SRV レコードを構成します。 **2.** Expressway-E ホスト名を Expressway-E のパブリック IP アドレスにポイントする A レコードを設定します。 （注） MRA エンドポイントは、Expressway-E に到達できるように、パブリック ドメインネームシステム（DNS）サーバーへの接続が必要です。 パブリック ドメインネームシステム（DNS）（外部ドメイン）を参照してください。 警告 Expressway-E の完全修飾ドメイン名（FQDN）は、SRV A レコードと一致して、MRA エンドポイントとパブリック ドメインネームシステム（DNS）サーバー間の接続を確立して、それらが Expressway-E に到達できるようにする必要があります。
ステップ6	Expressway-E 証明書を設定します。Expressway-E 証明書に各 Unified CM 登録ドメインが含まれていることを確認してください。 詳細については、証明書の要件を参照してください。
ステップ7	SAML SSO を展開している場合は、適切なドメインをアイデンティティプロバイダーに関連付けます。 IdP とドメインの関連付けを参照してください。

手順	タスク
ステップ 8	デバイス アクティベーションコードを使用して MRA クライアントをプロビジョニングする場合は、MRA導入準備のために Unified CM でクラスタ全体の MRA アクティベーション ドメインをプロビジョニングします。 さらに、デバイスがアクティブ化された後にユーザーが使用できるようにするエッジドメインを持つ MRA サービスドメインをプロビジョニングします。 MRA デバイス導入準備の構成フローを参照してください。

（オプション）SRV を使用して Expressway-E のエイリアス FQDN を作成する

複数のエッジドメインがある場合のオプションのアプローチは、SRV レコードを使用して、複数の Expressway-E FQDN をシミュレートする Expressway-E のエイリアスドメインを作成することです。たとえば、example.com に Expressway-E サーバーがあり、example.com と staging.com の 2 つのエッジドメインがある場合

- エッジドメインごとに、エッジドメインの一部であるかのように Expressway-E FQDN アドレスを指す _collab_edge SRV を構成します（例：expe.example.com を指す SRV や expe.staging.com を指す別の SRV）。
- FQDN ごとに、Expressway-E のパブリック IP アドレスを指す A レコードを設定します。

セッションの永続性

セッション持続性により、ローミング中のユーザーエクスペリエンスが向上し、Webex アプリで次のことができるようになります。

- ネットワーク内の異なるアクセスポイント間をローミングします。
- 再登録することなく、異なるネットワーク（Wi-Fi、VPN over 3G/4G など）間をローミングできます。
- 異なるネットワーク間をローミングしている間、SIP ベースのサブスクリプション ステータスを維持します。
- ネットワーク接続が失われた場合に備えて登録を維持します。
- アクティブな通話と保留中の通話の両方を、通話が途切れることなく、あるネットワークから別のネットワークにシームレスに転送します。

ネットワーク間のローミング中の接続を容易にするために、セッション持続性では、キープアライブ登録による動的な IP アドレス/ポートの変更が可能です。さらに、この機能には構成可能な TCP 再接続タイマーが含まれており、これは製品レベルで有効にする必要があり、一時的なネットワーク接続の切断またはローミングの場合に Webex アプリクライアントが接続を維持できるようにする必要があります。タイマーは、クライアントが元の TCP 接続を明示的

に切断した場合にのみ有効です。セッション持続性機能を利用するには、シスコ定義の SIP インターフェイスに準拠する必要があります。

たとえば、オフィス内で Webex アプリクライアントで通話中に、Wi-Fi 接続を失って建物の外に出た場合、クライアントが Expressway 経由でモバイルおよびリモートアクセスに切り替えると、通話は続行されます。同様に、クライアントが Expressway 経由でモバイルおよびリモートアクセスからオフィスの Wi-Fi ネットワークに切り替えても、通話が切断されることはありません。

Note セッション永続性機能にはソフトウェアの依存関係があり、Expressway での設定は必要ありませんが、機能が正しく動作するために CUCM でチェックするポリシーがあります。

以下は、ソフトウェアの依存関係です: **Wi-Fi から LTE へのコールハンドオフ**は、ソフトクライアントのエンドユーザーが、ネットワークの切り替え中にアクティブな通話を切断することなく、Wi-Fi ネットワークと LTE ネットワークを切り替えることができるようにします。Wi-Fi から LTE へのコールハンドオフ機能は自動的に有効になりますが、Unified Communications Manager リリース 14SU1 以降が必要です。

通話中に、ソフトクライアントがネットワークの変更を検出すると、登録の切り替えを行い、切り替えについてエンドユーザーに音声やビジュアルで表示してアクティブな通話を再接続します。ただし、ユーザーは、通話でシームレスなオーディオとビデオのエクスペリエンスを引き続き利用できます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。