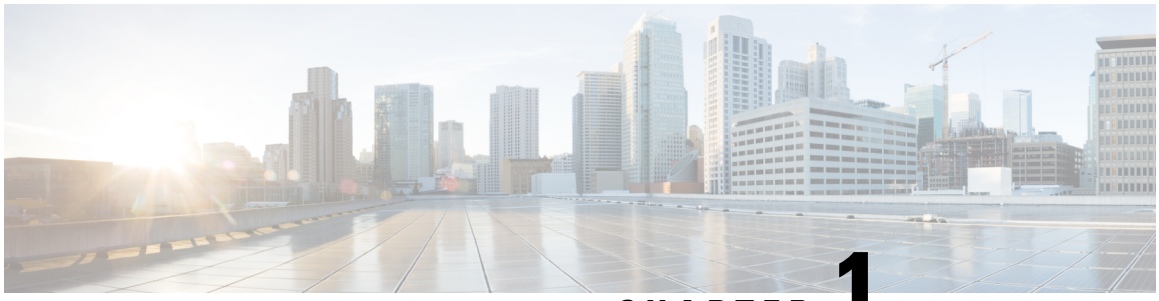
Cisco Expressway クラスタ作成と維持に関する導入ガイド（X14.3）

初版：2023 年 5 月 17 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



CHAPTER 1

このマニュアルについて

この章では、次の内容について説明します。

記載情報

バージョン X12.5 以降、このガイドは Cisco Expressway シリーズ製品（Expressway）にのみ適用され、Cisco VCS 製品（VCS）には適用されなくなりました。Cisco.com の古い VCS は、各ガイドのタイトルページで指定されている VCS バージョンで引き続き有効です。

本書では、次のトピックを説明します。

- クラスタリングの要件

  ピア Expressway をクラスタ化する前に必要なネットワーク環境と最小限の構成について説明します。

- クライアントの形成方法

  1 つのクラスタを形成し、クラスタにピアを追加し、必要に応じてクラスタアドレスマッピングを構成する方法。

- クラスタの変更方法

  アップグレード、ピアのオフライン化、プライマリピアの変更、クラスタの解除などのプロセス。

- Expressway クラスタを他のシステムに接続する方法

  Cisco TMS、他の Expressway、エンドポイントなどの外部システムにクラスタを接続する方法。

- トラブルシューティング

  クラスタが期待どおりに動作していない場合に役立つガイダンス。

- 参照先

ご使用の環境に関連する可能性のある追加資料。

クラスタ化されたシステムでのライセンスの使用状況とキャパシティの詳細については、[*Cisco Expressway* シリーズの維持と運用ガイド（Cisco Expressway Series Maintain and Operate Guides）] ページの『*Expressway* 管理者ガイド』を参照してください。

変更履歴

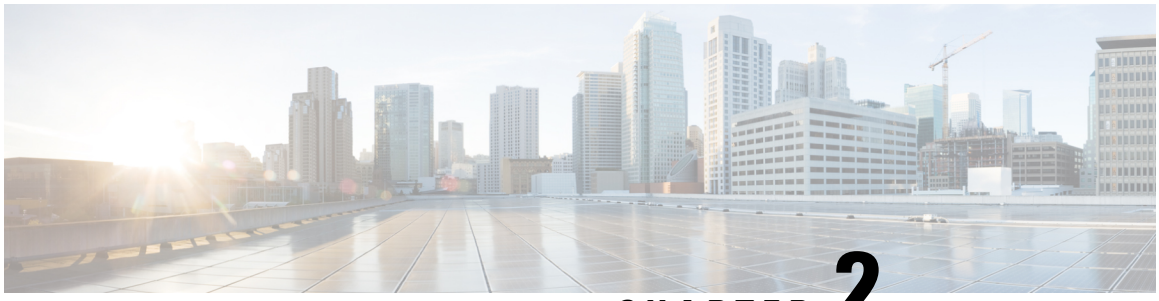
表 *1*：変更履歴

日付	変更内容	理由
2023 年 6 月	X14.3 リリースの初版 「（オプション）完全修飾ドメイン名を使用してクラスタを形成する」の章に「Expressway-E トラバーサルゾーンの使用上の注意」セクションを追加 「クラスタリング要件」の章の「クラスタ展開を Expressway と Expressway Select と混在する」セクションに注意事項を追加	X14.3 リリース
2021 年 7 月	X14.0.2 リリース用に更新。 いくつかの CDET に対応	X14.0.2 リリース
2021 年 4 月	X14.0 リリースの初版 「トラブルシューティング」の章にいくつかの「Expressway のアラームと警告」を追加	X14.0 リリース

日付	変更内容	理由
2020 年 6 月	• X12.6用に更新。また、現在は『*Expressway* 管理者ガイド』に記載されているクラスタライセンスの使用状況とキャパシティのガイドラインを削除。 • クラスタリング要件を更新して、B2B 展開のピアごとに A レコードまたは AAAA レコードを含む DNS SRV レコードの明確化を推奨。必須ではない。	X12.6 リリースおよび書類の訂正
2019 年 3 月	クラスタのピアを削除するとデュアル NIC 環境にある LAN2 インターフェイスのすべての構成が削除されることを明記	明記
2019 年 2 月	X12.5 用に更新。 このバージョンから、このガイドは Cisco Expressway シリーズにのみ適用され、Cisco VCS には適用されない。	X12.5 リリース
2019 年 2 月	クラスタアドレスマッピングを編集。ソフトウェアバージョンを X8.11.4 メンテナンスリリースに更新。テキストに対するその他の表面的な機能強化。	マニュアルの不具合、X8.11.4 リリース
2018 年 9 月	Webex と Spark プラットフォームのリブランド、CE1200 アプライアンス、および X8.11.1 メンテナンスリリースに応じて更新。	X8.11.1 リリース
2018 年 8 月	「クラスタ名と DNS SRV レコード」項のテキストと例を修正。	修正

日付	変更内容	理由
2018 年 7 月	X8.11 用に更新。	X8.11 リリース
2017 年 11 月	「前提条件」項のラウンドトリップ遅延と最大ホップ遅延を更新。	更新
2017 年 10 月	クラスタのアップグレード順序に関するアドバイスを強化。	明記
2017 年 8 月	すべてのクラスタピアを同じドメインで設定する必要があるという注記を追加。	中略
2017 年 7 月	X8.10 に関する内容を更新。	X8.10 リリース
2017 年 4 月	クラスタアドレスマッピングのセクションと関連する編集を追加。	X8.9.2 リリース
2016 年 12 月	TLS に関連する隔離されたネットワークのクラスタに関するセクションを追加。	X8.9 リリース
2016 年 6 月	クラスタ通信での TLS の使用開始。登録、FindMe、TMSPE のサポートが Expressway に導入。	X8.8 リリース
2015 年 11 月	X8.7 用に更新。	
2015 年 7 月	X8.6 用に更新。ピアを交換するための新しい手順。	
2015 年 4 月	X8.5 用にメニューパスを変更。X8.5.2 に合わせて再発行。	
2014 年 12 月	X8.5 用に更新。	
2014 年 6 月	X8.2 用に再発行。	

日付	変更内容	理由
2014 年 4 月	Expressway X8.1.1 を更新： • Expressway の新しい「クラスタのアップグレード」項 • Expressway ピアの交換の新しい項 • IP ポートとプロトコルの付録を更新	
2013 年 12 月	本書の Expressway バージョンの初回リリース。古い VCS バージョンは「VCS 構成ガイド」を参照。	



CHAPTER 2

クラスタリングの基本

この章では、次の内容について説明します。

概要

Expressway は最大 6 つの Expressway で構成されるクラスタに含めることができます。クラスタ内の各 Expressway がクラスタ内の他のすべての Expressway のピアです。クラスタ作成時に、1 つのピアをプライマリとして指定します。このプライマリピアの構成が他のピアに複製されます。

クラスタのすべての Expressway ピアのルーティングキャパシティは同じである必要があります。Expressway が通話を宛先にルーティングできる場合、そのクラスタのすべての Expressway ピアが、通話をその宛先にルーティングできると見なされます。ルーティングが異なる Expressway ピアで異なる場合は、個別の Expressway/Expressway クラスタを使用する必要があります。

クラスタリングの利点

クラスタ化された Expressway には、キャパシティと復元力の両方の利点があります。

- **キャパシティ**クラスタリングは、単一の Expressway と比べて Expressway 展開のキャパシティを最大 4 倍に増加させることができます。
- **復元力**。Expressway がメンテナンスモードでも、ネットワークの問題や停電またはその他理由によりアクセス不可になった場合でも、クラスタリングは冗長性を確保します。クラスタの Expressway ピアは、帯域幅の利用とルーティング、ゾーンおよびその他構成を共有します。エンドポイントは、クラスタの任意のピアに登録できます。よって、エンドポイントは、初期ピアと切断されても、クラスタ内の別のピアに再登録できます。

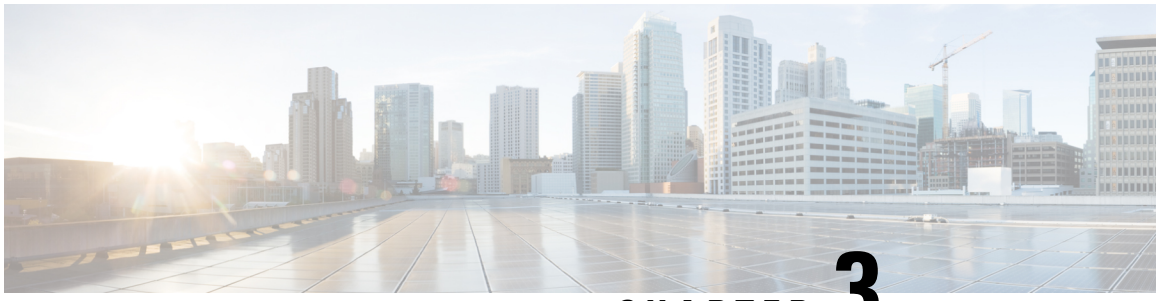
キャパシティゲインについて

キャパシティの増加につながるのは、4 つのピアまでです。たとえば 6 つのピアからなるクラスタでは、5 番目と 6 番目の Expressways はクラスタに通話キャパシティを追加しません。復元力はキャパシティではなく、ピアの追加によって強化されます。

Small Expressway VM は Cisco Business Edition 6000 のお客様を対象としているため、**Small VM のクラスタリングは冗長性のみを提供し**、追加のスケールメリットは提供しません。

ライセンスについて

キャパシティライセンスはクラスタ単位で実行され、クラスタピアにインストールされているすべてのキャパシティライセンスは、クラスタ内の任意のピアで使用できます。これには、リッチ メディア セッション ライセンスと、ルームシステムとデスクトップシステムの登録ライセンスが含まれます。詳細については、「クラスタ内でのライセンスの使用」を参照してください。



CHAPTER 3

クラスタリングの要件

Expressway ピアのクラスタを設定する前、またはクラスタに Expressway を追加する前に、次の要件が満たされていることを確認します。

この章では、次の内容について説明します。

Expressway-C と Expressway-E が混在しない

クラスタには、Expressway-C ノードのみ、または Expressway-E ノードのみを含める必要があります。同じクラスタ内で混在させることはできません。

プラットフォームとソフトウェアバージョンが一致

- すべてのクラスタピアが同じ Expressway ソフトウェアバージョンを実行している。異なるピアが異なるバージョンのコードを実行できる唯一の機会は、クラスタが分割された方法で動作する間に、クラスタが 1 つのバージョンのコードから他のバージョンのコードへアップグレードされる間です。
- 各ピアは、同等の機能を持つハードウェアプラットフォーム（アプライアンスまたは仮想マシン）を使用しています。たとえば、標準アプライアンスで実行されているピアと、2 コアの中規模 VM で実行されているピアをクラスタ化できますが、標準アプライアンスで実行されているピアと、8 コアの大規模 VM で実行されているピアをクラスタ化することはできません。

ネットワーク条件が満たされている

- 異なる LAN 設定（有効な異なる IPv4 アドレスと異なる IPv6 アドレス）が各ピアで設定されている。
- Expressway は、80 ミリ秒までのラウンドトリップ遅延をサポートします。つまり、クラスタ内の各 Expressway は、クラスタ内の他のすべてのピアから 40 ミリ秒以内である必要があります。
- クラスタの各ピアはクラスタ内またはクラスタに追加されるすべての Expressway に直接ルーティングできます。（クラスタ ピア間の NAT は許可されず、ファイアウォールがある場合、必須ポートがオープンであることを確認します）
- 外部ファイアウォールをクラスタリング TLS ポートへのアクセスをブロックするように構成されています。
- クラスタの形成中または手順の変更中、ピア間のネットワーク接続が信頼できるものである。

  クラスタリング手順は正しい順序で実行する必要があり、プライマリピアを最初に起動する必要があります。他のピアを最初に起動すると、クラスタの制御を引き継ぐことができ、その結果、回復が困難な一貫性のない構成状態が発生する可能性があります。

基本設定が完了した

- 各ピアは、他のすべてのピアに対して異なるシステム名を持ちます。
- 同じドメイン内のすべてのクラスタピアを構成します。
- 各ピアには、他のピアに対してピアを識別する証明書があります（**[TLS 検証モード（TLS Verification mode）]**のデフォルトが *[*許可（*Permissive*）*]* に設定されている場合は、最低限必要です）。

（注） 1 つのクラスタ内の複数の Expressway に 1 つの証明書を使用することはサポートされていますが、セキュリティリスクがあるため、これは推奨されません。つまり、1 つのデバイスで 1 つの秘密キーが侵害されると、クラスタ内のすべてのデバイスが侵害されます。

- 引き続きオプションキーを使用するシステムがある場合は、次の例外を除き、すべてのピアに同じオプションキーのセットがインストールされます。
  - RMS ライセンス
  - ルーム システムの登録ライセンス

- デスクトップ システム ライセンス登録

- 各ピアで H.323 モードを有効にします（**[構成（Configuration）]** > **[プロトコル（Protocols）]** > **[H.323]** の順に選択し、H.323 を *[オン（On）]* に設定）。

  クラスタは、すべてのエンドポイントが SIP エンドポイントであっても、ピア間の H.323 シグナリングを使用してコールの最適なルートを決定します。

- ピアを除くすべての IP アドレスからクラスタリング TLS ポートへの接続をブロックするように、各ピアでファイアウォールルールを構成します。

ドメインネームシステム（DNS）構成が完了した

DNS サーバー構成は複製されないため、各ピアで DNS サーバーアドレスを入力する必要があります。

- Expressway ピアで使用される DNS サーバーは、Cisco TMS およびすべての Expressway ピアアドレスの正引きおよび逆引き DNS 探索をサポートする必要があります。DNS サーバーは、次のような必要な他の DNS 機能のアドレスルックアップも提供する必要があります。
  - ドメインネームシステム（DNS）名を使用して構成した場合の NTP サーバーまたは外部マネージャ
  - Microsoft FE サーバーの FQDN ルックアップ
  - サーバーの正引きおよび逆引きルックアップ（逆引きルックアップは PRT レコードを介して頻繁に提供されます）

（注） Expressway-E は通常、パブリック ドメインネームシステム（DNS）を使用しますが、**プライベート** IP アドレスを解決するためにパブリック ドメインネームシステム（DNS）を使用することは望ましくありません。また、Expressway-E ピアのパブリックアドレスでクラスタ化することも望ましくありません。これらの理由から、クラスタアドレスマッピングを使用して、ピアの FQDN を**プライベート** IP アドレスに解決することをお勧めします。

詳細については、[Cisco Expressway シリーズ構成ガイド（Cisco Expressway Series Configuration Guides）] ページのご使用のバージョンに対応する『*Cisco Expressway* クラスタ作成および保守導入ガイド』を参照してください。

- DNS SRV レコードは、各ピアに A または AAAA レコードが含まれるクラスタに推奨されます。

  この構成は、ビデオの相互運用性とビジネスツービジネス（B2B）ビデオ通話には推奨されますが、**モバイルおよびリモートアクセス**には推奨されません。

- （MRA の場合）Expressway-E クラスタの各ピアに `collab-edge` SRV レコードを作成します。
- （B2B のみ）Expressway-E クラスタには、すべてのクラスタピアを定義する DNS SRV レコードがあります。

TMS が構成されている（必須の場合）

- Cisco TMS を使用している場合は、バージョン 13.2 以降で実行されています（プロビジョニングまたは FindMe に Cisco TMS を使用していない場合は、12.6 以降を使用できます）。
- Cisco TMS を FindMe またはプロビジョニングデータを複製するために使用する場合、[プロビジョニング拡張（Provisioning Extension）] モード機能を Cisco TMS で有効化します（詳細については、『Cisco TMS プロビジョニング拡張導入ガイド』を参照してください。）

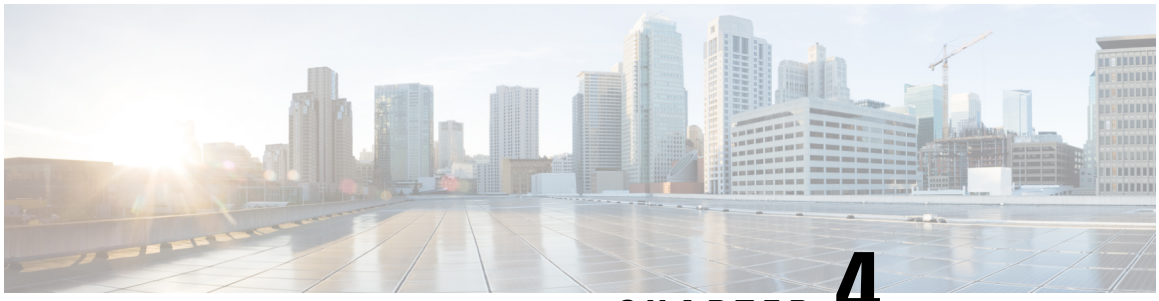
CE1200 および CE1100 物理アプライアンスが混在するクラスタ

CE1100 モデルが含まれている既存のクラスタに CE1200 アプライアンスを追加するには、クラスタに CE1200 を追加する前に、**[ステータス（Status）]** > **[概要（Overview）]** ページのサービスのセットアップウィザードを使用して、他のピアに合わせて [タイプ（Type）] オプションを構成します（Expressway-E または Expressway-C）。

アプライアンスタイプが混在するクラスタがある場合は、すべてのピアが同じソフトウェアバージョンを実行する必要があることに注意してください。**すべてのアプライアンスタイプがすべてのソフトウェアバージョンをサポートしているわけではありません。**まず、アプライアンスの設置ガイドで、混在させるユニットがすべて同じソフトウェアバージョンをサポートできることを確認してください。

クラスタ展開を Expressway と Expressway Select と混在する

（注） Expressway および Expressway Select ピアで構成される Expressway クラスタはサポートされていません。代わりに、クラスタ内のすべてのピアが Expressway ソフトウェアイメージまたは Expressway Select ソフトウェアイメージを実行する必要があります。



CHAPTER 4

クライアントの形成方法

この章では、次の内容について説明します。

概要

- クラスタには、プライマリを含めて最大 6 つの Expressway を設定できます。
- クラスタにピアを 1 つずつ追加します。
- 設定変更はプライマリ Expressway のみで行う必要があります。

⚠

注意 実行中のすべてのピアでクラスタが安定するまで、クラスタ全体の設定を変更しないでください。いずれかのピアがアップグレード中または再起動中である、あるいはサービスを使用できない状態でクラスタ設定の変更を行った場合、クラスタデータベースの複製により悪影響が及ぶ恐れがあります。

他のピアに対する変更がクラスタ全体に反映されることはなく、次にプライマリの設定がピア全体に複製された場合に上書きされます。一部のピア固有のアイテムについては例外です。

クラスタ内のすべてのピアに変更で更新されるまで、最大 1 分待つ必要があります。

- クラスタ通信障害アラームは、クラスタの形成中に発生します。終了すると、アラームはクリアされます。
- 新しい Expressway がクラスタに適切に参加する前に、構成の複製が中断されます。
- 新しい Expressway ピアに 2 つのネットワーク インターフェイスがある場合、**ピア *N* アドレス**で外部インターフェイスを指定することはできません。ピア間に TLS を適用する必要がある場合（つまり、TLS 検証が *ON* の場合）、ピア N アドレスのピアの証明書に記載されているピアの FQDN を使用する必要があります。FQDN のドメインネームシステム（DNS）解決はパブリック IP アドレスに解決される可能性があるため、クラスタアドレ

スマッピングも使用する必要があります。FQDN をプライベート IP アドレスにマッピングする方法については、Expressway-E クラスタのクラスタアドレスマッピングを参照してください。

- Expressway サーバーで単一の NIC と静的 NAT が有効になっている場合、**ピア *N* アドレス**を静的 NAT アドレスにすることはできません。ピア間に TLS を適用する必要がある場合（つまり、TLS 検証が *ON* の場合）、ピア N アドレスのピアの証明書に記載されているピアの FQDN を使用する必要があります。FQDN のドメインネームシステム（DNS）解決はパブリック IP アドレスに解決される可能性があるため、クラスタアドレスマッピングも使用する必要があります。FQDN をプライベート IP アドレスにマッピングする方法については、Expressway-E クラスタのクラスタアドレスマッピングを参照してください。

クラスタに参加するための Expressway の準備

- 必要に応じて、新しいピアをサービス外にします。
  1. メンテナンスモードを有効化し（**[メンテナンス（Maintenance）]**>**[メンテナンスモード（Maintenance mode）]**）、このピアですべての通話がクリアされ、登録がタイムアウトするまで待機します。
  2. Expressway がクラスタ内にある場合は、既存のクラスタから削除してから再起動します。
  3. Expressway を初期設定にリセットします（前の手順で再起動したため、この操作をまだ行っていない場合）。
- Expressway のアドレスが組織内の他の Expressway のピアではないことを確認します。
- Expressway が他の Expressway のネイバー、トラバーサルクライアント、またはトラバーサルサーバーでないことを確認します。
- Expressway が次のように構成されているかを再確認し、修正します。
  - 適切なイーサネット速度（**[システム（System）]** > **[ネットワーク インターフェイス（Network interfaces）]** > **[イーサネット（Ethernet）]**）。
  - 有効な IP アドレスおよび IP ゲートウェイ（**[システム（System）]** > **[ネットワーク インターフェイス（Network interfaces）]** > **[IP]**）。
  - 有効で稼働している NTP サーバーが構成されている（[ステータス（Status）]セクションで、**[システム（System）]** > **[時間（Time）]**、**[状態（State）]** が「[同期（Synchronized）]」に設定されている）。
  - 少なくとも 1 つの有効な DNS サーバーが構成されている。また、非修飾 DNS 名が（NTP サーバーなどで）使用されている場合、**ドメイン名**が正しく構成されている必要があります（**ドメイン名**は、FQDN とするために、非修飾 DNS 名のサフィックスとして追加されます）（**[システム（System）]** > **[DNS]**）。

- **[システム（System）]** > **[DNS]** の順に選択し、**[システムのホスト名（System host name）]** がこの Expressway の DNS ホスト名であることを確認します（通常は、スペースを除き、**[システム（System）]** > **[管理（Administration）]** の **[システム名（System name）]** と同じであり、クラスタの各 Expressway で一意です）。正しく構成されていない場合は、適切に構成して、**[保存（Save）]** をクリックします。

（注） <System host name>.<DNS domain name> = この Expressway の FQDN

- ピアが構成されていない（**[システム（System）]**>**[クラスタリング（Clustering）]**ーこのページのすべての [ピア N アドレス（Peer N address）] フィールドは空欄にする必要があります。）

注意 クラスタリングページからすべてのピアアドレスフィールドをクリアして設定を保存した場合、Expressway を次に再起動したときに、自動的に Expressway が初期設定にリセットされます。つまり、LAN1 インターフェイスの基本的なネットワーク設定を除き、既存の設定のすべてを失うことになります。これには、フィールドをクリアしてから次に再起動するまでに行ったすべての設定も含まれます。

この Expressway がすでにクラスタのメンバーである場合は、別のクラスタで使用する前に、そのクラスタから削除して再起動する必要があります。

- オプションキーを使用するシステムがある場合は、クラスタの他のすべてのピアにインストールされるオプションキー（**[メンテナンス（Maintenance）]**>**[オプションキー（Option keys）]**）と同じオプションキーのセットがインストールされていることを確認します。通話/RMS/デバイス/ロームライセンスの数は、ピアごとに異なる場合があります。そのたすべてのライセンスキーは、各ピアで同じである必要があります。
- **[H.323 モード（H.323 Mode）]** を [オン（On）] に設定（**[構成（Configuration）]**>**[プロトコル（Protocols）]** > **[H.323]**）

- この Expressway が Cisco TMSPE と統合されているクラスタに参加している場合は、Cisco TMS に Expressway を追加。

1. 新しい Expressway が Cisco TMS を認識できることを確認します。

   これを行うには、**[システム（System）]**>**[外部マネージャ（External manager）]** の順に選択し、**[ステータス（Status）]** セクションで、**[状態（State）]** が [アクティブ（Active）] であることを確認します。

2. Cisco TMS が Expressway のホスト名を認識していることを確認します。

   1. **[システム（Systems）]** > **[ナビゲータ（Navigator）]**（および必須サブフォルダ）の順に選択します。

2. この Expressway を選択します。
3. **[接続（Connection）]** タブを選択します。
4. **[ホスト名（Host Name）]** を、vcs3.uk.company.com など、この下位ピアの FQDN に設定します。
5. [保存/試行（Save/Try）] をクリックします。

   「`DNS config failure resolving <DNS name>: Did not find system IP address () in DNS: <Server IP>`」 などのエラーメッセージは無視します。
6. Cisco TMS が ドメインネームシステム（DNS）を更新することを確認します。
   1. [設定（Settings）] タブを選択します。
   2. **[強制的に更新（Force Refresh）]** をクリックします。
7. Cisco TMS が新しい Expressway と通信できることを確認します。

   これを行うには、Cisco TMS で **[システム（System）]** > **[ナビゲータ（Navigator）]**（および必要なサブフォルダ）の順に選択し、Expressway の名前をクリックして、次のように表示されていることを確認します。

   「✓システムにオープンチケットまたは確認済みチケットがありません」

- **[システム（System）]** > **[アラーム（Alarms）]** の順に選択します。Expressway の再起動を促すアラームが表示された場合、**[メンテナンス（Maintenance）]** > **[再起動（Restart）]** オプション の順に選択し、**[再起動（Restart）]** をクリックします。

Expressway ピアの新しいクラスタの作成

このプロセスでは、1 つの Expressway のクラスタを開始します。クラスタがすでにある場合は、このプロセスを使用しないでください。

重要 他のピアを追加する前に、まず1つの（プライマリ）ピアのクラスタを作成し、プライマリを再起動する必要があります。「1つのクラスタ」を確立した後に、さらにピアを追加できます。

1. プライマリピアにする Expressway を決定します。プライマリ Expressway は、クラスタのすべての Expressway ピアの構成情報のソースとして使用されます。下位の Expressway ピアでは、ほとんどの構成が削除され、プライマリの構成に置き換えられます。
2. Expressway が X12.6 ソフトウェアを実行していることを確認します。
3. Expressway をバックアップします（**[メンテナンス（Maintenance）]** > **[バックおよびリストア（Backup and restore）]**）。
4. Expressway が次のように構成されているかを再確認し、修正します。

- 適切なイーサネット速度（**[システム（System）]** > **[ネットワーク インターフェイス（Network interfaces）]** > **[イーサネット（Ethernet）]**）
- 有効な IP アドレスおよび IP ゲートウェイ（**[システム（System）]** > **[ネットワーク インターフェイス（Network interfaces）]** > **[IP]**）。
- 有効で稼働している NTP サーバーが構成されている（**[ステータス（Status）]**セクションで、**[システム（System）]** > **[時間（Time）]**、[状態（State）] が 「[同期（Synchronized）]」 に設定されている）。
- 少なくとも 1 つの有効な DNS サーバーが構成されている。また、非修飾 DNS 名が（NTP サーバーなどで）使用されている場合、**ドメイン名**が正しく構成されている必要があります（**ドメイン名**は、FQDN とするために、非修飾DNS名のサフィックスとして追加されます）（**[システム（System）]** > **[DNS]**）。
- **[システム（System）]** > **[DNS]** の順に選択し、**[システムのホスト名（System host name）]** がこの Expressway の DNS ホスト名であることを確認します（通常は、スペースを除き、**[システム（System）]** > **[管理（Administration）]** の **[システム名（System name）]** と同じであり、クラスタの各 Expressway で一意です）。正しく構成されていない場合は、適切に構成して、**[保存（Save）]** をクリックします。

（注） <System host name>.<DNS domain name> = この Expressway の FQDN

- ピアが構成されていない（**[システム（System）]** > **[クラスタリング（Clustering）]** ー このページのすべての [ピア N アドレス（Peer N address）] フィールドは空欄にする必要があります。）

注意 クラスタリングページからすべてのピアアドレスフィールドをクリアして設定を保存した場合、Expressway を次に再起動したときに、自動的に Expressway が初期設定にリセットされます。つまり、LAN1インターフェイスの基本的なネットワーク設定を除き、既存の設定のすべてを失うことになります。これには、フィールドをクリアしてから次に再起動するまでに行ったすべての設定も含まれます。

このExpresswayがすでにクラスタのメンバーである場合は、別のクラスタで使用する前に、そのクラスタから削除して再起動する必要があります。

- オプションキーを使用するシステムがある場合は、クラスタの他のすべてのピアにインストールされるオプションキー（**[メンテナンス（Maintenance）]** > **[オプションキー（Option keys）]**）と同じオプションキーのセットがインストールされていることを確認します。通話/RMS/デバイス/ロームライセンスの数は、ピアごとに異なる場合があります。そのたすべてのライセンスキーは、各ピアで同じである必要があります。

- **[H.323 モード（H.323 Mode）]** を *[オン（On）]* に設定（**[構成（Configuration）]** > **[プロトコル（Protocols）]** > **[H.323]**）

5. このExpresswayのリストに、ネイバーゾーンまたはトラバーサルゾーンの新しいクラスタのピアとする Expressway が表示されていないことを確認します（**[構成（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** で、各ネイバーおよびトラバーサルゾーンを確認します）。

6. **[ライブにする H.323 時間（H.323 Time to Live）]** を展開のサイズに適した値に設定します。60（秒）などの小さい数値は、1 つの Expressway がアクセス不能になった場合に、エンドポイントが別のピアにすぐに登録することを意味します（**[構成（Configuration）]** > **[プロトコル（Protocols）]** > **[H.323]**）。

（注） 登録の存続時間を短縮しすぎると、登録要求が Expressway へ大量に送り付けられるリスクがあり、パフォーマンスに重大な影響を及ぼします。この影響はエンドポイントの数に比例します。したがって、パフォーマンスを良好に保つ必要性に対して、不定期に発生するフェールオーバーの必要性とのバランスをとることが必要です。

7. **[システム（System）]** > **[DNS]** の順に選択し、**[システムのホスト名（System host name）]** がこの Expressway の DNS ホスト名であることを確認します（通常は、スペースを除き、**[システム（System）]** > **[管理（Administration）]** の **[システム名（System name）]** と同じであり、クラスタの各 Expressway で一意です）。正しく構成されていない場合は、適切に構成して、**[保存（Save）]** をクリックします。

（注） <System host name>.<DNS domain name> = この Expressway の FQDN

8. **[構成（Configuration）]** > **[コールルーティング（Call routing）]** の順に選択し、**[コールシグナリングの最適化（Call signaling optimization）]** を *[オン（On）]* にします。

9. **[Save]** をクリックします。

10. メンテナンスモードを有効化し（**[メンテナンス（Maintenance）]** > **[メンテナンスモード（Maintenance mode）]**）、このピアですべての通話がクリアされ、登録がタイムアウトするまで待機します。

11. （MRA 展開には適用されません）**[システム（System）]** > **[クラスタリング（Clustering）]** の順に選択し、**クラスタ名**が、この Expressway クラスタをアドレス指定している SRV レコードで使用されているルート可能な完全修飾ドメイン名であることを確認します。例えば、`cluster1.example.com`。（クラスタ名と DNS SRV レコードを参照してください。）

    必要に応じて **[クラスタ名（Cluster name）]** を変更します。

12. **[Save]** をクリックします。

13. 次のように、**[クラスタリング（Clustering）]** ページでフィールドを構成します。

構成プライマリ	1
クラスタ IP バージョン	基盤となるネットワーク アドレッシング スキームに合わせて、*IPv4* または *IPv6* を選択します。
TLS 検証モード	オプション：*[許可（Permissive）]*（デフォルト）または *[強制（Enforce）]*。 *[許可（Permissive）]* は、クラスタ内 TLS 接続を確立するときにピアが互いの証明書を検証しないことを意味します。 *[強制（Enforce）]* はより安全ですが、各ピアに有効な証明書があり、署名 CA が他のすべてのピアによって信頼されている必要があります。 次のように、FQDN および TLS 検証を使用してクラスタを形成することを推奨します。*[許可（Permissive）]* モードで IP アドレスを使用してクラスタを形成し、ピアアドレスを FQDN に変更します。その後、TLS 検証モードを *[強制（Enforce）]* に切り替えることができます。 隔離されたネットワークで Expressway-E ピアをクラスタリングする場合は、クラスタアドレスマッピングも構成する必要があります。詳細な手順については、Expressway-E クラスタのクラスタアドレスマッピングを参照してください。
ピア 1 アドレス	この Expressway（プライマリピア）のアドレスを入力します。 **[TLS 検証モード（TLS verification mode）]** が *[強制（Enforce）]* に設定されている場合は、このピアの証明書のサブジェクト CN または SAN と一致する FQDN を入力する必要があります。

14. [**Save**] をクリックします。

    [ピア 1 アドレス（Peer 1 address）] フィールドの右に、「*This system*」 が表示されます（表示前にページを更新する必要がある場合があります）。

15. Expressway を再起動します（**[メンテナンス（Maintenance）]** > **[リスタートオプション（Restart options）]** の順に選択し、**[リスタート（Restart）]** をクリックし、**[OK]** をクリックします）。

16. 構成データが想定どおりに存在することを確認します。

    - FindMe を使用している場合、想定っされる FindMe エントリが既存しているか確認します（**[ステータス（Status）]** > **[アプリケーション（Applications）]** > **[TMS プロビジョニング拡張サービス（TMS Provisioning Extension Services）]** > **[FindMe]** > **[アカウント（Accounts）]**）。

- **[システム（System）]**、**[構成（Configuration）]**、**[アプリケーション（Application）]** メニューで、各項目の構成を確認します。

17. デフォルトでは、[メンテナンス（Maintenance）] モードは無効です。
    1. **[メンテナンス（Maintenance）]** > **[メンテナンスモード（Maintenance mode）]** の順に選択します。
    2. **[メンテナンスモード（Maintenance mode）]** を *[オフ（Off）]* に設定します。
    3. [**Save**] をクリックします。
18. Expressway をバックアップします（**[メンテナンス（Maintenance）]** > **[バックアップおよびリストア（Backup and restore）]**）。

これで、（1 つの Expressway の）クラスタの形成が完了しました。

次のステップ

- **[ステータス（Status）]** > **[アラーム（Alarms）]** の順に選択し、すべてのアラームが機能し、クリアされていることを確認します。
- クラスタにピアを追加を使用して、他の Expressway をクラスタに追加します。

クラスタにピアを追加

この手順では、（1 つ以上のピアからなる）既存の X12.6 クラスタに新しいピアを追加し、プライマリピアの構成を Expressway に複製します。

既存のクラスタがない場合は、Expressway ピアの新しいクラスタの作成を参照してください。

1. プライマリ Expressway で、**[システム（System）]** > **[クラスタリング（Clustering）]** の順に選択します。

   1 つ以上の **[ピア *N* アドレス（Peer N address）]** フィールドが空欄になっているはずです。
2. 1 つ目の空欄フィールドに、新しい Expressway ピアのアドレスを入力します。
3. [**Save**] をクリックします。

   ピア 1 は、「This system」と表示します。新しいピアは、「Unknown」を表示する場合があり、リフレッシュすると、「Failed」と表示します。これは、まだクラスタに完全に追加されていないからです。
4. クラスタ内にすでに存在する下位ピアのいずれかで**[システム（System）]**>**[クラスタリング（Clustering）]** の順に選択し、次のフィールドを編集します。

クラスタ名	プライマリ Expressway で構成されている**クラスタ名**と同じもの

設定プライマリ	プライマリ Expressway で選択したものと同じ番号
クラスタ IP バージョン	プライマリ Expressway で選択したものと同じバージョン
TLS 検証モード	プライマリ Expressway で選択したものと同じ設定*
Peer 1 address …Peer 6 address	アドレスは、プライマリ Expressway で入力したアドレスと同じで、同じ順序である必要があります。

*クラスタアドレスマッピングを使用する場合は、クラスタ内のすべてのデバイスを最初に [許可（Permissive）] モードにする必要があります。詳細については、Expressway-E クラスタのクラスタアドレスマッピングを参照してください。

新しいクラスタリング構成を**保存**します。

5. クラスタ内にすでに存在する下位ピアごとに、前の手順を繰り返します。
6. 新しいピアで、**[システム（System）]** > **[クラスタリング（Clustering）]** の順に選択します。

クラスタ名	プライマリ Expressway で構成されている**クラスタ名**と同じもの
設定プライマリ	プライマリ Expressway で選択したものと同じ番号
クラスタ IP バージョン	プライマリ Expressway で選択したものと同じバージョン
TLS 検証モード	プライマリ Expressway で選択したものと同じ設定*
Peer 1 address …Peer 6 address	アドレスは、プライマリ Expressway で入力したアドレスと同じで、同じ順序である必要があります。

*クラスタアドレスマッピングを使用する場合は、クラスタ内のすべてのデバイスを最初に [許可（Permissive）] モードにする必要があります。詳細については、Expressway-E クラスタのクラスタアドレスマッピングを参照してください。

新しいクラスタリング構成を**保存**します。

7. Expressway はクラスタ通信障害アラームを生成します。アラームは、必要な再起動後にクリアされます。

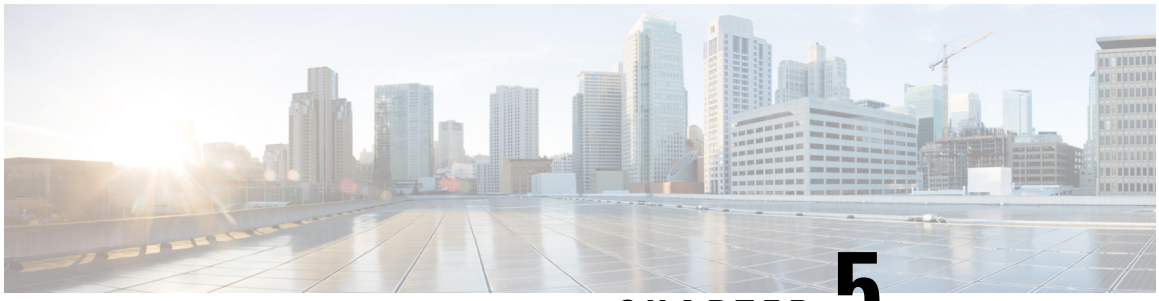
8. Expressway を再起動します（**[メンテナンス（Maintenance）]** > **[リスタートオプション（Restart options）]** の順に選択し、**[リスタート（Restart）]** をクリックし、**[OK]** をクリックします）。

チェック

1. リスタート後、約 2 分間待ちます。この間に、プライマリから構成がコピーされます。
2. クラスタ データベース ステータスを確認します。
3. 構成データが想定どおりに存在することを確認します。
   - FindMe を使用している場合、想定っされる FindMe エントリが既存しているか確認します（**[ステータス（Status）]** > **[アプリケーション（Applications）]** > **[TMS プロビジョニング拡張サービス（TMS Provisioning Extension Services）]** > **[FindMe]** > **[アカウント（Accounts）]**）。
   - **[システム（System）]**、**[構成（Configuration）]**、**[アプリケーション（Application）]** メニューで、各項目の構成を確認します。

次のステップ

- 必要に応じてピアを追加します。
- クラスタで Conference Factory（Multiway™）を使用している場合は、他の Expressway アプリケーションでのクラスタリングの影響を参照してください。
- ピアで FQDN をプライベート IP アドレスに解決する場合は、Expressway-E クラスタのクラスタアドレスマッピングを参照してください。



CHAPTER 5

（オプション）完全修飾ドメイン名を使用したクラスタの形成

この章では、ピアが FQDN を使用してクラスタを形成するように、IP アドレスを使用して形成されたクラスタを変更する方法について説明します。これは、ピア間で TLS 検証を適用する場合に必要です。クラスタをまだ形成していない場合は、クライアントの形成方法を参照してください。

Expressway-E のクラスタを作成する場合、それらは DMZ などの隔離されたネットワークにある可能性があり、TLS 検証を適用する場合はローカルマッピングを使用する必要があります。Expressway-C のクラスタを形成している場合は、クラスタアドレスマッピングを使用する必要はありません。

この章では、次の内容について説明します。

Expressway-E クラスタのクラスタアドレスマッピング

MRA などのセキュアな展開では、各 Expressway-E ピアに、パブリック FQDN を含む SAN の証明書が必要です。FQDN は、パブリック ドメインネームシステム（DNS）で Expressway-E のパブリック IP アドレスにマッピングされます。この構成により、MRA エンドポイントなどの外部エンティティが Expressway-E のパブリックインターフェイスを検出し、セキュアな接続を確立できます。

クラスタアドレスマッピングが必要な場合

- Expressway-E ピアをクラスタ化するだけで、ピア間の TLS 検証が必要ない場合は、ノードのプライベート IP アドレスを使用してクラスタを形成できます。クラスタアドレスマッピングは不要です。

- クラスタ内の Expressway-E ピアが証明書を使用して互いの ID を確認できるようにする場合は、ドメインネームシステム（DNS）を使用してクラスタピア FQDN をパブリック IP アドレスに解決することを許可できます。これは、Expressway-E ノードに NIC が 1 つだけあり、静的 NAT を使用せず、ルーティング可能な IP アドレスがある場合に、クラスタ形成を完全に許可する方法です。クラスタアドレスマッピングは不要です。
- セキュリティポリシーでピア間の TLS 検証を強制することが指定されている場合、および Expressway-E が静的 NAT またはデュアル NIC、あるいはその両方を使用している場合は、外部インターフェイスまたは静的 NAT アドレスを使用してクラスタを形成することは推奨されません。

  また、外部接続が切断されるため、パブリック ドメインネームシステム（DNS）を使用してピアのパブリック FQDN をプライベート IP アドレスにマッピングしないでください。

  このような状況では、クラスタアドレスマッピングを使用する必要があります。

クラスタアドレスマッピングの仕組み

完全修飾ドメイン名を使用してクラスタを形成する場合、ピアはそれらの名前を IP アドレスに変換できる必要があります。この変換がドメインネームシステム（DNS）の主な理由ですが、ピアがドメインネームシステム（DNS）にアクセスできない場合、または FQDN をプライベート IP アドレスに変換する必要がある場合は、クラスタ アドレス マッピング テーブルに入力して、ドメインネームシステム（DNS）のローカル代替を提供できます。

クラスタアドレスマッピングは、クラスタ全体で共有される FQDN:IP ペアです（ピアごとに 1 ペア）。ピアは、ドメインネームシステム（DNS）にクエリする前にマッピングテーブルをクエリし、一致が見つかった場合はドメインネームシステム（DNS）を照会しません。

TLS を適用する場合、ピアは互いの証明書の SAN フィールドから名前を読み取り、マッピングの FQDN 側に対して各名前を確認する必要があります。SAN がマッピングの FQDN 側と一致し、証明書を提示した IP アドレスがマッピングの IP 側と一致する場合、ピアは他のピアを信頼し、TLS 接続を確立できます。

ドメインネームシステム（DNS）を使用しない場合、クラスタアドレスマッピングは、この検証を実現する唯一の方法です。

提案されたマッピングの取得元

IP アドレスを使用してクラスタがすでに形成されており **[システム（System）]** > **[DNS]** ページで構成されている**システムホスト名**と DNS 名がすでにピアにある場合、次のように想定されるマッピングをクラスタ アドドレス マッピング テーブルに自動入力するオプションがあります。

```
<Peer1 Private IP address> にマッピングされる Peer1Hostname.Peer1DNSName

….

<Peer6 Private IP address> にマッピングされる Peer6Hostname.Peer6DNSName
```

（注） **この自動マッピングは正しくない可能性があります。**ピアの証明書の SAN フィールドに想定される FQDN が含まれていない場合、**[TLS 検証モード（TLS verification mode）]** が *[強制（Enforce）]* に変更されたときにクラスタは形成されません。ピア FQDN フィールドに入力したエントリが SAN に含まれていることを確認する必要があります。

クラスタアドレスマッピングの構成（Expressway-E クラスタ）

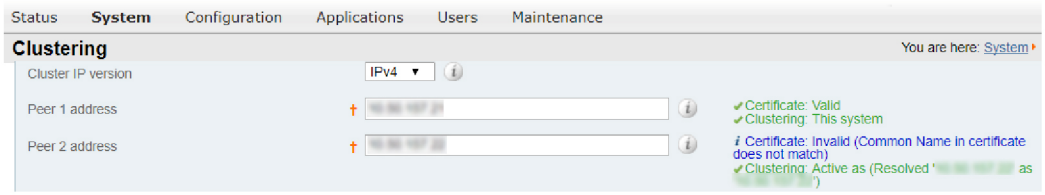
プライマリピアでマッピングを入力することを強く推奨します。アドレスマッピングは、クラスタを介して動的に複製されます。

マッピングの順番は重要ではありませんが、アドレスマッピングを使用する場合、**プライベート** IP アドレスのみを使用して、各クラスタピアに対してマッピングを作成する必要があります。

ステップ 1 **[TLS 検証モード（TLS verification mode）]** を *[許可（Permissive）]* に設定し、IP アドレス（Expressway ピアの新しいクラスタの作成 （16 ページ） および クラスタにピアを追加 （20 ページ） で説明あり）を使用してクラスタを形成します。

ステップ 2 [ピアアドレス（Peer Address）] フィールドに対して緑色のクラスタリング ステータス メッセージをチェックして、クラスタが正しく形成されていることを確認します。

また、青色の *Certificate: Invalid* ...status メッセージも表示されます。これは、FQDN によってピアを識別するように正しく形成されていると仮定すると、証明書が内部/プライベート IP アドレスに対応してはならないためです。これは予期される動作であり、続行を妨げるものではありません。



ステップ 3 プライマリピアで、**[システム（System）]**>**[クラスタリング（Clustering）]** の順に選択し、**[クラスタアドレスマッピングを有効化（Cluster address mapping enabled）]** ドロップダウンを *[オン（On）]* に変更します（デフォルトは、*[オフ（Off）]* です）。

[クラスタアドレスマッピング（Cluster address mapping）] フィールドが表示されます。

ステップ 4 （オプション、上記の注を参照）**[システム情報に基づいてマッピングを提案する（Suggest mappings based on system information）]** をクリックして、各クラスタピアのマッピングフィールドに自動入力します。こ

れは、各ピアの [システム（System）] > [DNS] ページで設定された**システムホスト名**と **DNS 名**を使用し、それらを内向きの NIC の IP アドレスにマッピングします。

ステップ 5 （自動入力オプションを使用した場合）推奨されるマッピングが、ピアの証明書の名前、およびクラスタ化する NIC の IP アドレスに対応していることを確認します。（データは、証明書またはドメインネームシステム（DNS）と一致しない可能性がある情報から作成されます）。

ステップ 6 Expressway-E ピアのパブリック FQDN が内部 NIC の IP アドレスに対応するようにマッピングを編集します。

（証明書の [SAN] フィールドでパブリック FQDN を確認するか、ドメインネームシステム（DNS）を照会することで確認できます）。

ステップ 7 [**Save**] をクリックします。

マッピングが保存され、他のクラスタピアにコピーされます。

（注） クラスタは引き続き IP アドレスを使用して形成されており、TLS 検証の *[*許可（*Permissive*）*]* モードを使用しています。**[ピア N アドレス（Peer N address）]** フィールドをパブリック FQDN に変更し、**[TLS 検証モード（TLS verification mode）]** を *[*強制（*Enforce*）*]* に変更すると、クラスタはこれらのマッピングの使用を開始します。

FQDN を使用するようにクラスタを変更

このトピックでは、IP アドレスを FQDN に置き換えて、ピアアドレスを体系的に変更する方法について説明します。次のアドレスに移動する前に、クラスタ全体で一度に 1 つのピアアドレスを変更できます。

FQDN を使用するように Expressway-E クラスタを変更するには、マッピングテーブルに入力されているアドレスを使用します（Expressway-E クラスタのクラスタアドレスマッピング （23 ページ） を参照）。

（注） ピアアドレスを変更している間、ピア間の通信は一時的に影響を受け、変更が完了してクラスタが新しいアドレスに同意するまでアラームが表示されます。

ステップ 1 すべてのクラスタピアにサインインし、**[システム（System）]** > **[クラスタリング（Clustering）]** の順に選択します。

ステップ 2 最初に変更するピアアドレスを選択します。リスト内のすべてのピアアドレスに対して次のプロセスを 1 つずつ繰り返す必要があるため、**ピア 1 アドレス**から開始することをお勧めします。

ステップ 3 クラスタ内のすべてのピアで、次の手順を実行します。

- 選択した [ピアアドレス（peer address）] フィールドを IP アドレスから対応する FQDN に変更します（マッピングを行った場合は、この段階ですべてのピアで複製する必要があります）。

- [**Save**] をクリックします。

注意　　各ボックスでピアアドレスを 1 つだけ変更してください。

ステップ 4 現在変更しているピアアドレスによって識別されるピアに切り替え、このピアを再起動します（**[メンテナンス（Maintenance）] > [再起動（Restart）] オプション** の順に選択し、**[再起動（Restart）] > [OK]** の順に選択します。）。

（注）　　すべてのピアでピアアドレスを変更する場合は、1 回再起動する必要があります。

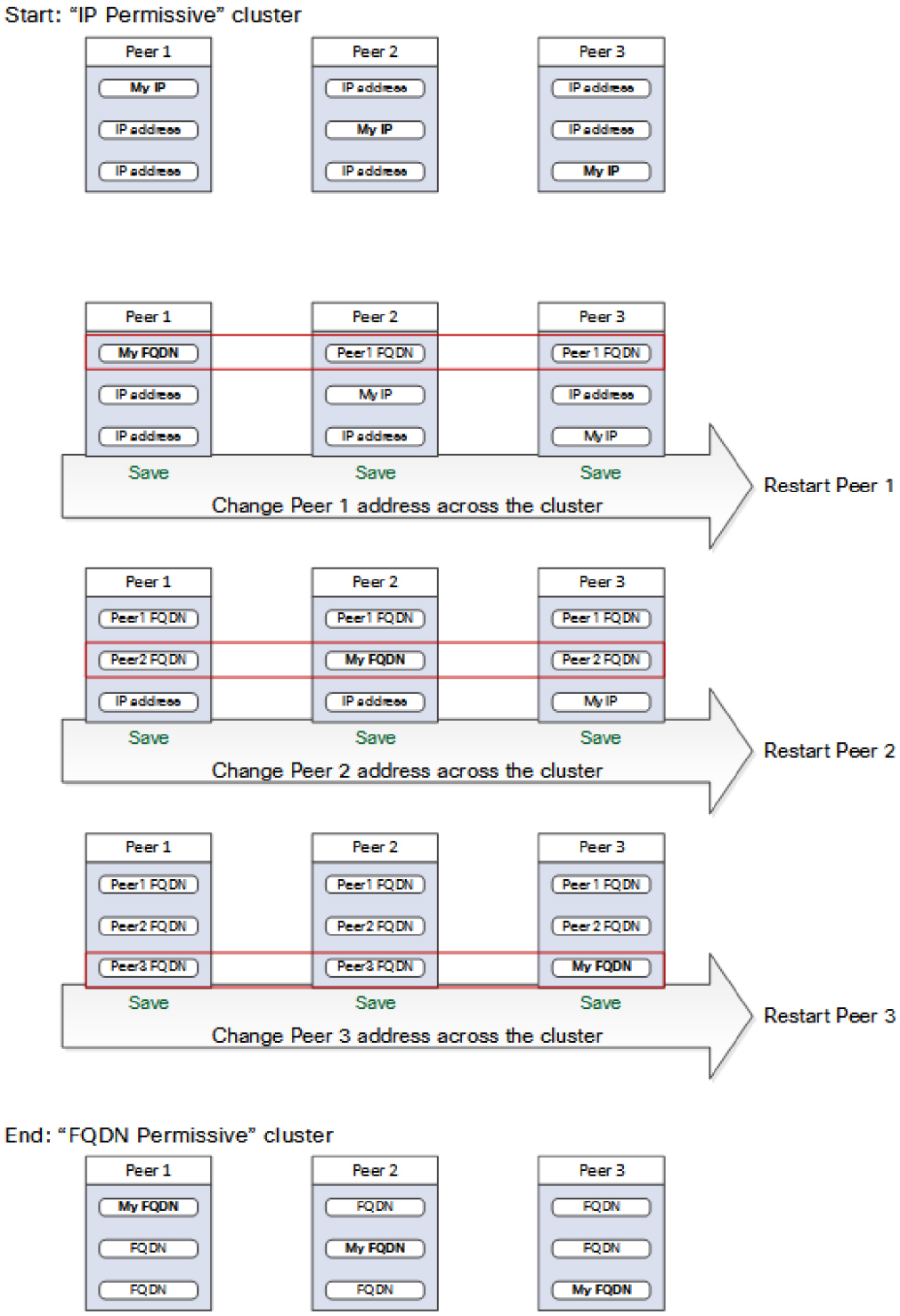
ステップ 5 一時的なクラスタリングアラームが解決するまで待機します。

クラスタ全体で、このピアのクラスタリングアドレスが IP アドレスから FQDN に正常に変更されます。

ステップ 6 次に変更するピアアドレスを選択し、ステップ 3 ～ 5 を繰り返します。すべてのピアアドレスを変更し、すべてのピアを再起動するまで、このループを繰り返します。

これでクラスタ全体が FQDN で動作し、クラスタは *[*許可（*Permissive*）*]* モードのままになります。

クラスタが Expressway-E クラスタであり、ピア間で TLS 検証を適用することを目的としている場合、[ピアアドレス（Peer Address）] フィールドは証明書に示されている ID と一致する必要があります。クラスタリングと証明書の両方のステータスメッセージが緑色であることを確認します。


Start: “IP Permissive” cluster
Peer 1
My IP
IP address
IP address
Peer 2
IP address
My IP
IP address
Peer 3
IP address
IP address
My IP
Peer 1
My FQDN
IP address
IP address
Peer 2
Peer1 FQDN
My IP
IP address
Peer 3
Peer1 FQDN
IP address
My IP
Save
Save
Save
Change Peer 1 address across the cluster
Restart Peer 1
Peer 1
Peer1 FQDN
Peer2 FQDN
IP address
Peer 2
Peer1 FQDN
My FQDN
IP address
Peer 3
Peer1 FQDN
Peer2 FQDN
My IP
Save
Save
Save
Change Peer 2 address across the cluster
Restart Peer 2
Peer 1
Peer1 FQDN
Peer2 FQDN
Peer3 FQDN
Peer 2
Peer1 FQDN
Peer2 FQDN
Peer3 FQDN
Peer 3
Peer1 FQDN
Peer2 FQDN
My FQDN
Save
Save
Save
Change Peer 3 address across the cluster
Restart Peer 3
End: “FQDN Permissive” cluster
Peer 1
My FQDN
FQDN
FQDN
Peer 2
FQDN
My FQDN
FQDN
Peer 3
FQDN
FQDN
My FQDN
445424

TLS 検証の適用

はじめる前に

⚠

注意 証明書 SAN に、[ピア N アドレス（Peer N address）] フィールドの FQDN が含まれていることを確認します。続行する前に、各アドレスフィールドの横にクラスタリングと証明書の緑色のステータスメッセージが表示されます。

TLS 検証の適用プロセス

ステップ 1 プライマリピアで、**[TLS 検証モード（TLS verification mode）]** を *[*強制（*Enforce*）*]* に設定します。

注意 いずれかの証明書が無効である場合は警告が表示され、強制 TLS 検証モードでクラスタが正常に動作しなくなります。

新しい TLS 検証モードは、クラスタ全体に複製されます。

ステップ 2 **[TLS 検証モード（TLS verification mode）]** が各ピアで [強制（Enforce）] になっていることを確認します。

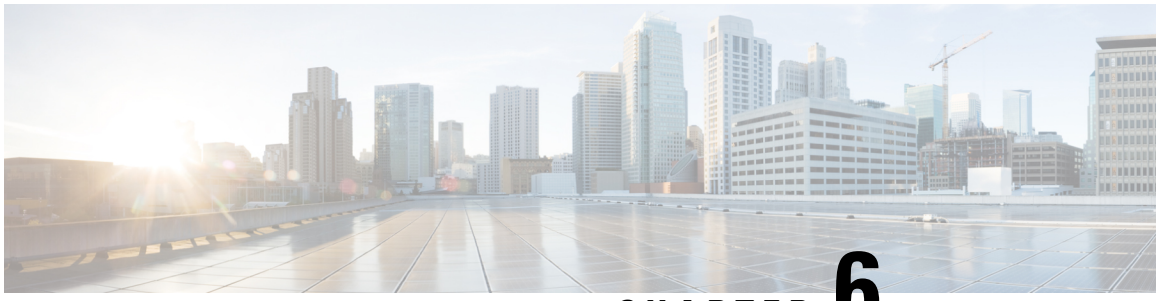
ステップ 3 **[保存（Save）]** をクリックし、プライマリピアを再起動します。

ステップ 4 他のピアにサインインしてから、ピアを再起動します。

ステップ 5 クラスタが安定するまで待ち、すべてのピアのクラスタリングと証明書のステータスが緑色であることを確認します。

Expressway-E トラバーサルゾーンの使用上の注意

これは、初期設定ではなく運用上の使用方法に関するものですが、ここでは便宜上提供しています。Expressway-C クラスタの FQDN は、Expressway-E トラバーサルゾーンの [TLS 検証サブジェクト名（TLS verify subject name）] フィールドで構成する必要があることに注意してください。Expressway は SAN 属性（サブジェクト代替名）を使用して、CN（共通名）ではなく、受信した証明書を検証します。



CHAPTER 6

クラスタの変更方法

クラスタが他のシステムに接続されている場合、クラスタへの変更は統合システムに影響を与える可能性があります。クラスタを変更する場合は、次の点に注意してください。

- このクラスタのネイバー、クライアント、またはサーバーである他の Expressway を確認し、ゾーン構成を更新します。たとえば、このクラスタにピアを追加または削除するときに、このクラスタに対するネイバーゾーンのピアアドレス一覧を更新する必要があります。
- クラスタと統合する他のシステムへの接続を確認します。たとえば、Cisco Unified Communications Manager にクラスタへのトランクがある場合や、新しいクラスタピアで更新する必要がある自動生成された MRA ゾーンがある場合があります。
- Expressway クラスタに登録されているエンドポイントが新しいピアまたは削除されたピアを認識していることを確認し、変更されたクラスタのピアに等しく登録されるようにします。
- ピアを追加または削除する場合、または IP アドレスまたは FQDN を変更する場合は、このクラスタのドメインネームシステム（DNS）エントリを変更します。
- Expressway 物理アプライアンスを使用する場合：
  - CE1100 モデルが含まれている既存のクラスタに CE1200 アプライアンスを追加するには、クラスタに CE1200 を追加する前に、**[ステータス（Status）] > [概要（Overview）]** ページのサービスのセットアップウィザードを使用して、他のピアに合わせて [タイプ（Type）] オプションを構成します（Expressway-E または Expressway-C）。

    クラスタ内の既存のアプライアンスよりも新しいモデルを追加する場合は、後で新しいアプライアンスに復元するバックアップを作成する前に、既存のピアの Expressway ソフトウェアを新しいアプライアンスと同じバージョンにアップグレードします。（バックアップは、作成されたのと同じソフトウェアバージョンにのみ復元できます）。**すべてのアプライアンスタイプがすべてのソフトウェアバージョンをサポートしているわけではありません。**まず、アプライアンスの設置ガイドで、混在させるユニットがすべて同じソフトウェアバージョンをサポートできることを確認してください。

- SAML メタデータを再エクスポートし、IDP にコピーします。Expressway-C のクラスタでピアを追加、削除、または交換するたびに、クラスタの SAML メタデータを変更します。クラスタが MRA 接続クライアントの SSO 用に構成されている場合、クラスタの新しい SAML メタデータで IDP を更新するまで、SSO が失敗することがあります。これは、ピアの（一意の）シリアル番号がクラスタのメタデータの生成に使用されるためです。詳細については、[Expressway 構成ガイド（Expressway configuration guides）] ページの『*Cisco Expressway* 経由のモバイルおよびリモートアクセス導入ガイド』を参照してください。

Note クラスタ全体の SAML メタデータでは、メタデータをエクスポートするだけでは不十分です。すべての Expressway クラスタピアの FQDN 情報を含む SAML 証明書を再生成する必要があります。

Note クラスタを新しいソフトウェアバージョンにアップグレードする手順については、該当するバージョンのリリースノートを参照してください。

この章では、次の内容について説明します。

クラスタを変更する前に

- ピアとして設定されるシステムを、互いにネイバーとして設定することはできません。
- ピアがさまざまな LAN に導入されている場合、ピア間の遅延の程度が低くなるよう、ネットワーク間に十分な接続性を確保する必要があります。
- クラスタ ピアは個別のサブネットに配置することができます。ピアは、サブネット境界を越えて送信される H.323 メッセージングを使用して互いに通信します。
- 同じ LAN にクラスタ内のすべてのピアを導入すると、ローカル ドメイン名やローカル ドメイン サブネット マスクなど、同じルーティング情報を使用して設定できます。
- クラスタからピアを削除するには、そのピアのすべてのピア アドレス フィールドをクリアして設定を保存した後、再起動する必要があります。

⚠

注意 クラスタリングページからすべてのピアアドレス フィールドをクリアして設定を保存した場合、Expressway を次に再起動したときに、自動的に Expressway が初期設定にリセットされます。つまり、LAN1 インターフェイスの基本的なネットワーク設定を除き、既存の設定のすべてを失うことになります。これには、フィールドをクリアしてから次に再起動するまでに行ったすべての設定も含まれます。

Expresswayに、初期設定へのリセットが保留中であることを通知するバナーが表示されます。

初期設定にリセットさせないためには、クラスタリング ピアアドレス フィールドを以前とまったく同じ状態に復元します。元のピア アドレスを同じ順序で置き換えてから設定を保存すると、バナーがクリアされて、リセットが防止されます。

ライブピアをクラスタから永久削除

このプロセスでは既存のクラスタから 1 つの Expressway ピアを削除します。

- クラスタ全体を解除する場合は、代わりに「クラスタの解除 （37 ページ）」を参照してください。
- プライマリピアを削除する場合は、このピアを削除する前に別のピアをプライマリにします。プライマリピアの変更 （38 ページ）を参照してください。
- 削除するピアにアクセスできない場合は、「クラスタからデッドピアを永久削除 （35ページ）」を参照してください。
- Expressway クラスタピアを回復する場合は、「Expressway クラスタピアのリカバリ （37 ページ）」を参照してください。

クラスタから削除する Expressway 上

ステップ 1 **[システム（System）]** > **[クラスタリング（Clustering）]** の順に選択します。

ステップ 2 **[ピア *N* アドレス（Peer N address）]** フィールドのすべてのエントリを削除します。

ステップ 3 保存します。

注意 クラスタリングページからすべてのピアアドレス フィールドをクリアして設定を保存した場合、Expressway を次に再起動したときに、自動的に Expressway が初期設定にリセットされます。つまり、LAN1 インターフェイスの基本的なネットワーク設定を除き、既存の設定のすべてを失うことになります。これには、フィールドをクリアしてから次に再起動するまでに行ったすべての設定も含まれます。

初期設定へのリセットを避ける必要がある場合は、クラスタリング ピアのアドレス フィールドを以前と同じ状態に復元してください。元のピア アドレスを同じ順序で置き換えてから、設定を保存してバナーをクリアしてください。

ステップ 4 Expressway を再起動します（**[メンテナンス（Maintenance）]**>**[リスタートオプション（Restart options）]** の順に選択し、**[リスタート（Restart）]** をクリックし、**[OK]** をクリックします）。

ピアが再起動すると、初期設定へのリセットが自動的にトリガーされ、機密データとクラスタリング設定が削除されます。リセットによって、次に示す基本的なネットワーク情報を除くすべての構成がクリアされます。これは、引き続き Expressway にアクセスできるようにするために LAN1 インターフェイスに対して保存されます。デュアル NIC オプションを使用する場合は、すべての LAN2 設定がリセットによって完全に削除されることに注意してください。

リセット後に保持される構成（LAN1 用）：

- IP アドレス
- 管理者および root アカウントおよびパスワード
- SSH キー
- オプション キー
- HTTPS アクセスが有効
- SSH アクセス有効（SSH Access Enabled）

（注） バージョン X12-6 以降、工場出荷時の状態にリセットすると、サーバー証明書、関連付けられた秘密キー、および CA 信頼ストア設定がピアから削除されます。以前の Expressway ソフトウェアバージョンでは、これらの設定は保持されていました。

プライマリ Expressway 上

ステップ 1 **[システム（System）]** > **[クラスタリング（Clustering）]** の順に選択します。

ステップ 2 削除された Expressway のアドレスを削除します。

ステップ 3 削除する Expressway が、リストの最後のフィールドでない場合、エントリ間に空のフィールドができないように、リスト上の他のアドレスが上に移動します。

ステップ 4 前述の手順で、プライマリ Expressway ピアの IP アドレスがリスト上で上に移動した場合、その新しい位置に合わせて **[構成プライマリ（Configuration primary）]** の値を変更します。

ステップ 5 [保存（Save）] をクリックします。

残りのすべての下位 Expressway ピア

ステップ 1 **[システム（System）]** > **[クラスタリング（Clustering）]** の順に選択します。

ステップ 2 **[ピア N アドレス（Peer N address）]** フィールドと **[構成プライマリ（Configuration primary）]** フィールドを編集して、プライマリ Expressway で構成されているものと同じにします。

ステップ 3 [**Save**] をクリックします。

ステップ 4 残りすべての下位 Expressway ピアで、クラスタリング構成が同じになるまで、この手順を繰り返します。

クラスタからライブ Expressway が削除されます。

クラスタからデッドピアを永久削除

この手順では、サービス外ピアを RMAd にする必要がある場合、またはその他の理由でアクセスできない場合に、クラスタからそのピアを削除します。

- クラスタ全体を解除する場合は、「クラスタの解除 （37ページ）」を参照してください。
- 削除するピアにアクセスできる場合は、「ライブピアをクラスタから永久削除 （33 ページ）」を参照してください。
- プライマリピアを削除する場合は、このピアを削除する前に別のピアをプライマリにします。「プライマリピアの変更 （38 ページ）」を参照してください。
- Expressway クラスタピアを回復する場合は、「Expressway クラスタピアのリカバリ （37 ページ）」を参照してください。

（注） この手順では、Expressway から構成はクリアされません。システムを復活させることができた場合は、デフォルト設定をリセットする（工場出荷時の状態へのリセット）まで、そのシステムを使用しないでください。

プライマリ Expressway で、次の手順を実行します。

1. **[システム（System）]** > **[クラスタリング（Clustering）]** の順に選択します。
2. 削除された Expressway のアドレスを削除します。
3. 削除する Expressway が、リストの最後のフィールドでない場合、エントリ間に空のフィールドができないように、リスト上の他のアドレスが上に移動します。
4. 前述の手順で、プライマリ Expressway ピアの IP アドレスがリスト上で上に移動した場合、その新しい位置に合わせて **[構成プライマリ（Configuration primary）]** の値を変更します。
5. [**Save**] をクリックします。

残りのすべての下位 Expressway ピアで、次の手順を実行します。

1. **[システム（System）]** > **[クラスタリング（Clustering）]** の順に選択します。
2. [**ピア *N* アドレス**（Peer N address）] フィールドと **[構成プライマリ（Configuration primary）]** フィールドを編集して、プライマリ Expressway で構成されているものと同じにします。
3. [**Save**] をクリックします。
4. 残りすべての下位 Expressway ピアで、クラスタリング設定が同じになるまで、この手順を繰り返します。

Expressway クラスタからアクセスできないピアを削除しました。

このピアから構成をクリア

削除するピアを復元する場合、ネットワークに接続する前に構成をクリアする必要があります。

ステップ 1 **[システム（System）]** > **[クラスタリング（Clustering）]** の順に選択します。

ステップ 2 **[ピア N アドレス（Peer N address）]** フィールドのすべてのエントリを削除します。

ステップ 3 [**Save**] をクリックします。

ステップ 4 Expressway を再起動します（**[メンテナンス（Maintenance）]**>**[リスタートオプション（Restart options）]** の順に選択し、**[リスタート（Restart）]**をクリックし、**[OK]**をクリックします）。再起動すると、Expressway は初期設定へのリセットを開始します。次を除くすべての構成が削除された状態で復元します。

ピアが再起動すると、初期設定へのリセットが自動的にトリガーされ、機密データとクラスタリング設定が削除されます。リセットによって、次に示す基本的なネットワーク情報を除くすべての構成がクリアされます。これは、引き続き Expressway にアクセスできるようにするために LAN1 インターフェイスに対して保存されます。**デュアル NIC オプションを使用する場合は、すべての LAN2 設定がリセットによって完全に削除される**ことに注意してください。

リセット後に保持される構成（LAN1 用）：

- IP アドレス
- 管理者および root アカウントおよびパスワード
- SSH キー
- オプション キー
- HTTPS アクセスが有効
- SSH アクセス有効（SSH Access Enabled）

（注） バージョン X12-6 以降、工場出荷時の状態にリセットすると、サーバー証明書、関連付けられた秘密キー、および CA 信頼ストア設定がピアから削除されます。以前の Expressway ソフトウェアバージョンでは、これらの設定は保持されていました。

これで、クラスタに戻すことができます。クラスタにピアを追加 （20 ページ） を参照してください。

Expressway クラスタピアのリカバリ

Expressway はクラスタ内にあります。意図せずにクラスタから削除されたピアを元の位置に再挿入することはできません。このような状況では、以下を実行します。

- 再挿入する前に、クラスタからピアを削除する
- クラスタリストの最後のピアにする
- このようなピアのバックアップは、再挿入後にクラスタリストで異なる完全修飾ドメイン名（FQDN）を持つため、役に立たなくなります。

クラスタの解除

このプロセスは既存のクラスタからすべての Expressway ピアを削除します。FindMe および構成レプリケーションが停止します。また、プロビジョニングも停止し、クラスタが Cisco TMS から削除されます。

各 Expressway は、Web インターフェイスにアクセスするのに十分な構成を保持しますが、他のすべての構成はクリアされます。

この手順では、ピアを 1 つずつ削除し、最後にプライマリピアからクラスタリング構成をクリアします。X8.11 以降では、クラスタリング構成をクリアすると、Expressway を工場出荷時の状態にリセットする準備ができます。Expressway を「1 つのクラスタ」として構成する必要がある場合があるため、プライマリを初期設定にリセットする必要があります。

クラスタの解除方法

ステップ 1 アクセスできないピアを削除します。「クラスタからデッドピアを永久削除 （35 ページ）」を参照してください。

ステップ 2 Cisco TMSPE を使用している場合は、Cisco TMS にサインインし、クラスタへのプロビジョニングを停止します。

1. **[システム（Systems）]** > **[ナビゲータ（Navigator）]**（および必須サブフォルダの順に選択し、クラスタの Expressway をクリックします。
2. **[プロビジョニング（Provisioning）]** タブを選択します。
3. すべての 4 つのサービスを無効にします（チェックボックスをオフにします）。
4. **[Save]** をクリックします。

ステップ 3 各下位ピアを削除します。「ライブピアをクラスタから永久削除 （33 ページ）」を参照してください。

最後の下位ピアを削除する場合は、プライマリピアだけをクラスタに残す必要があります。

クラスタは「1 つのクラスタ」になり、この Expressway をその構成で保持する場合は、ここで終了できます。

ステップ 4 プライマリピアを初期設定にリセットする場合は、プライマリピアにサインインし、ライブピアをクラスタから永久削除 （33 ページ） のプロセスに従います。

クラスタの解除は完了です。

プライマリピアの変更

現在のプライマリピアにアクセスできない場合でも、このプロセスを実行できます。複数のピアがプライマリとして競合している状態にクラスタを置かないように、ここに記載されている順序で手順を実行してください。

通常は、プライマリ Expressway ユニットをサービス外にする場合、または元のプライマリピアに障害が発生した場合にのみ、**プライマリ構成**を変更する必要があります。

（注） Cisco TMS の変更はありません。Cisco TMS は、Expressway クラスタのプライマリ変更を確認して適切に報告します。

ステップ 1 「新規」プライマリ Expressway で、**[システム（System）]** > **[クラスタリング（Clustering）]** の順に選択します。

ステップ 2 [構成プライマリ（Configuration primary）] ドロップダウンメニューで、「This system」と記載のあるピアエントリの ID 番号を選択します。

ステップ 3 **[Save]** をクリックします。

プライマリピアを変更する場合、「クラスタマスター不一致（Cluster master mismatch）」または「クラスタ レプリケーション エラー（Cluster replication error）」というアラームが 表示されますが、この手順の実行中に修正されるので無視してください。

ステップ 4 他のすべての Expressway ピアで、「古い」プライマリピアから開始して（まだアクセス可能な場合）、**[システム（System）]** > **[クラスタリング（Clustering）]** の順に選択します。

ステップ 5 [構成プライマリ（Configuration primary）] ドロップダウンメニューで、「新しい」プライマリ Expressway の ID 番号を選択します。

ステップ 6 **[Save]** をクリックします。

Expressway ピアで発生した「クラスタマスター不一致（Cluster master mismatch）」および「クラスタ レプリケーション エラー（Cluster replication error）」に関するアラームは、約 2 分後に自動的にクリアされます。

ステップ 7 **[システム（System）]>[クラスタリング（Clustering）]** の順に選択し、ページを更新して、**[構成プライマリ（Configuration primary）]** への変更が適用されていることを確認します。

ステップ 8 Expressway で変更が適用されていない場合は、上記の手順を繰り返します。

ステップ 9 クラスタデータベースのステータスがアクティブであることを確認します。

ステップ 10 「古い」プライマリピアにアクセスできないためにプライマリピアを変更する場合は、「クラスタからデッドピアを永久削除 （35 ページ）」の手順を参照してください。

ステップ 11 「古い」プライマリを復活させる場合は、他のピアから分離し、可能であれば初期設定にリセットする必要があります。

有効なクラスタアドレスマッピングが設定されている FQDN を使用している場合、これ以上の手順は必要ありません。

ピア ID の変更

Expressway ピアの IP アドレス、ホスト名、または完全修飾ドメイン名（FQDN）を変更するには、クラスタから Expressway を削除し、その IP アドレス、ホスト名、または FQDN を変更してから、Expressway をクラスタに戻す必要があります。

そのプロセスは次のとおりです。

ステップ 1 IP アドレス、ホスト名、または FQDN を変更する Expressway がプライマリ Expressway でないことを確認します。

プライマリ Expressway の場合は、プライマリピアの変更 （38 ページ） の手順に従って別のピアをプライマリにします。

ステップ 2 「ライブピアをクラスタから永久削除 （33 ページ）」で記載されているプロセスを実行します。

ステップ 3 Expressway の IP アドレスまたは FQDN を変更します。

ステップ 4 「クラスタにピアを追加 （20 ページ）」で記載されているプロセスを実行します。

デュアル NIC で Expressway-E を使用していて、外部 NIC の IP アドレス、ホスト名、または FQDN を変更する場合、クラスタリングにこの IP アドレス、ホスト名、または FQDN は使用されないので、クラスタリングを解除する必要はありません。

ピアの交換

このセクションでは、異なるユニットでクラスタピア Expressway を交換するための手順の概要を示します。

ステップ 1 交換する Expressway がプライマリ Expressway でないことを確認します。

プライマリ Expressway の場合は、プライマリピアの変更 （38 ページ） の手順に従って別のピアをプライマリにします。

ステップ 2 次のように、クラスタから既存のピアを削除します。

1. 交換するクラスタピアにアクセスできない場合、「クラスタからデッドピアを永久削除 （35 ページ）」で定義した手順を実行します。
2. 交換するクラスタピアにアクセスできる場合、「ライブピアをクラスタから永久削除 （33 ページ）」で定義した手順を実行します。

ステップ 3 「クラスタにピアを追加 （20 ページ）」で定義されている手順を使用して、交換ピアをクラスタに追加します。

重要 物理アプライアンスを含むクラスタがある場合の追加情報

CE1100 モデルが含まれている既存のクラスタに CE1200 アプライアンスを追加するには、クラスタに CE1200 を追加する前に、**[ステータス（Status）] > [概要（Overview）]** ページのサービスのセットアップウィザードを使用して、他のピアに合わせて [タイプ（Type）] オプションを構成します（Expressway-E または Expressway-C）。

クラスタ内の既存のアプライアンスよりも新しいモデルを追加する場合は、後で新しいアプライアンスに復元するバックアップを作成する前に、既存のピアの Expressway ソフトウェアを新しいアプライアンスと同じバージョンにアップグレードします。（バックアップは、作成されたのと同じソフトウェアバージョンにのみ復元できます）。すべてのアプライアンスタイプがすべてのソフトウェアバージョンをサポートしているわけではありません。まず、アプライアンスの設置ガイドで、混在させるユニットがすべて同じソフトウェアバージョンをサポートできることを確認してください。

ピアの交換とその構成の移行

この手順では、アクセス可能な Expressway ピアを別の Expressway に置き換えることを前提としています。

ステップ 1 交換する Expressway がプライマリ Expressway でないことを確認します。

プライマリ Expressway の場合は、プライマリピアの変更 （38 ページ） の手順に従って別のピアをプライマリにします。

ステップ 2 **クラスタリング構成を削除してピアを削除しますが、まだ再起動しないでください。**「ライブピアをクラスタから永久削除 （33 ページ）」を参照してください。

ステップ 3 再起動する前に、削除したピアの構成をバックアップします。

ステップ 4 必要に応じて、新しい Expressway に必要なオプションキーを生成して適用します。他のピアに適用されるのと同じキーのセットを適用します。

ステップ 5 削除したピアから新しい Expressway にバックアップを復元します。

ステップ 6 新しい Expressway のドメインネームシステム（DNS）構成が他のピアと同じであることを確認し、同じ NTP サーバーと同期します。

ステップ 7 クラスタにピアを追加 （20 ページ） で定義されている手順を使用して、交換ピアをクラスタに追加します。

この手順を実行する場合は、削除されたピアのアドレスの代わりに新しいピアのアドレスを使用する必要があります。

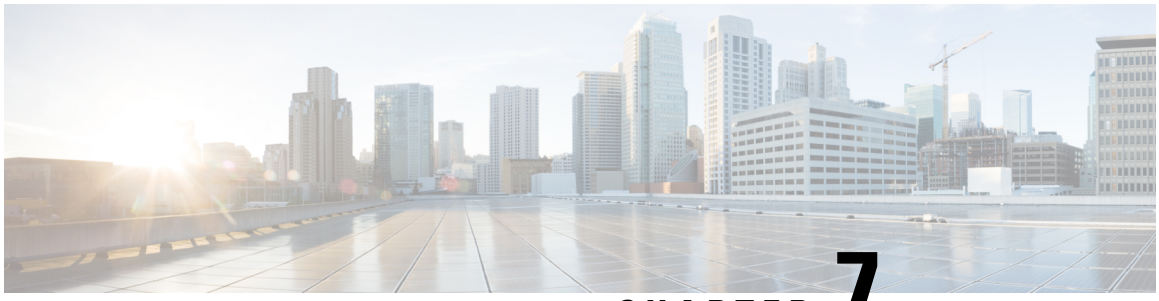
最も重要な手順を次に示します。

1. 古いピアのアドレスの代わりに、プライマリのクラスタリング構成に新しいピアのアドレスを追加します。
2. 古いピアのアドレスの代わりに、他の既存のピアのクラスタリング構成に新しいピアのアドレスを追加します。
3. 新しいピアに新しいクラスタリング構成（クラスタ名、共有秘密、順序付きピアリスト）を入力します。

ステップ 8 新しいピアを再起動します。

ステップ 9 約 5 分間待ってから、クラスタのステータスを確認し、アラームを解決します。

ステップ 10 削除したピアを再起動して初期設定へのリセットを開始し、古い構成をクリアします。



CHAPTER 7

Expressway クラスタを他のシステムに接続する方法

この章では、次の内容について説明します。

Expressway クラスタ間の隣接化

ローカル Expressway クラスタをリモートクラスタに隣接させることができます。リモートクラスタは、ローカルシステムへのネイバー、トラバーサルクライアント、またはトラバーサルサーバなどです。ローカルの Expressway でコールを受信し、関連するゾーンを経由してリモートクラスタに渡された場合、ネイバークラスタのリソース使用率が最も低いピア（メンテナンスモードのピアは考慮されません）にルーティングされます。そのピアは、コールを次のいずれかの方法に転送します。

- エンドポイントがそのピアに登録されている場合のローカルで登録されたエンドポイント
- エンドポイントがクラスタの別のピアに登録されている場合のピア
- エンドポイントが他の場所にある場合の外部ゾーン

構成手順については、『*Expressway* 管理者ガイド』を参照してください。

クラスタで機能するようにエンドポイントを構成

エンドポイントを構成するときは、クラスタ内のすべての Expressway ピアについて知っていることが理想です。そのため、初回登録時以降、エンドポイントが Expressway ピアへの接続を失った場合、クラスタ内の別のピアに登録できます。このセクションでは、SIP エンドポイントと H.323 エンドポイントにそれぞれ使用可能な構成方法を（推奨される順序で）示します。

DNS SRV およびラウンドロビン DNS の詳細については、『*Expressway* 管理者ガイド』の「URI ダイヤリング」項および「クラスタ名と DNS SRV レコード （61 ページ）」を参照してください。

（注） SIP エンドポイントと H.323 エンドポイントの動作は異なります。

SIP エンドポイント

1 つ以上の Expressway クラスタピアにアクセスできなくなった場合に、Expressway のクラスタへのエンドポイントの接続性のレジリエンスを提供するために、オプションが優先設定順に一覧されます。選択するオプションは、使用するエンドポイントがサポートする機能により異なります。

オプション 1 – SIP アウトバウンド（推奨）

重要 Cisco Collaboration Endpoint ソフトウェアで実行中のエンドポイントの場合、このオプションは、バージョン CE8.0 以降はサポートされません。

SIP アウトバウンドでは、エンドポイントを複数の Expressway ピアに同時に登録できるように構成できます。これによる利点として、エンドポイントとピア間の接続が失われた場合でも、エンドポイントと他のピアが引き続き接続されることが挙げられます。両方のピアに同時に登録しているエンドポイントでは、登録の失敗を別のピアに登録する前に認識するので、サービスは中断しません。そのため、エンドポイントは到達不能になりません。

SIP アウトバウンドの設定は、エンドポイントにより異なりますが、通常、次のように設定します。

- プロキシ 1
  - [サーバ検出（Server discovery）] = [手動（Manual）]
  - サーバーアドレス=クラスタピアのドメインネームシステム（DNS）名またはクラスタピアの IP アドレス
- プロキシ 2
  - [サーバ検出（Server discovery）] = [手動（Manual）]
  - サーバーアドレス=別のクラスタピアのドメインネームシステム（DNS）名または別のクラスタピアの IP アドレス
- [アウトバウンド（Outbound）] = [オン（On）]

オプション 2 – DNS SRV（2 番目に推奨）

このオプションを使用するには、各クラスタピアで同じウェイトと優先順位を定義する Expressway クラスタの DNS 名で使用できる DNS SRV レコードが必要です。

各 SIP エンドポイントで、[SIP 設定（SIP Settings）] を次のように設定します。

- [サーバ検出（Server discovery）] = [手動（Manual）]
- サーバーアドレス = Expressway クラスタのドメインネームシステム（DNS）名

エンドポイントが DNS SRV をサポートする場合、エンドポイントは起動時に DNS SRV 要求を送信して、各クラスタ ピアで同じウェイトと優先順位を定義する DNS SRV レコードを受け取ります。

次に、エンドポイントは、関連するクラスタ ピアへの登録を試行します（優先順位とウェイトが考慮されます）。このピアが使用でいない場合、エンドポイントは、同じ優先順位の別のピアへの登録を試行します。同じ優先順位のすべてのピアで登録を試行すると、次に優先順位の低いピアへの登録を試行します。これは、エンドポイントが Expressway に登録できるまで繰り返されます。

エンドポイントは、最初に登録した Expressway を再登録および通話に使用します。エンドポイントは、その Expressway との接続を失った場合、DNS SRV エントリを使用して、優先順位の高い Expressway から、登録先の新しい Expressway を探します。

ドメインネームシステム（DNS）トラフィックを最小限にするため、DNS SRV キャッシュタイムアウトを 24 時間など、比較的長時間に設定する必要があります。

オプション 3 – DNS ラウンドロビン（3 番目に推奨）

このオプションを使用するには、IP アドレスのラウンドロビン リストを提供する Expressway クラスタの DNS 名で使用できる DNS A レコードが必要です。

各 SIP エンドポイントで、[SIP 設定（SIP Settings）] を次のように設定します。

- [サーバ検出（Server discovery）] = [手動（Manual）]
- サーバーアドレス = Expressway クラスタのドメインネームシステム（DNS）名

エンドポイントが DNS SRV をサポートしない場合、エンドポイントは起動時に、DNS A レコード ルックアップを実行します。DNS サーバは、各クラスタ ピア メンバーをラウンドロビン リストに定義し、ラウンドロビン DNS をサポートするように設定されます。

エンドポイントは、DNS ルックアップにより提供されたアドレスを使用し、関連するクラスタ ピアへの登録を試行します。そのアドレスが使用できない場合、エンドポイントは、もう一度 DNS 探索を実行して、提供される新しい Expressway ピアへの接続を試行します（DNS サーバは、次のクラスタ ピアの IP アドレスを提供します）。これは、エンドポイントが Expressway に登録できるまで繰り返されます。

エンドポイントは、最初に登録した Expressway を再登録および通話に使用します。エンドポイントは、その Expressway との接続を失うと、もう一度 DNS 探索を実行して、登録先の新し

い Expressway を探します（DNS サーバーは、Expressway をラウンドロビン方式で提供します）。

ドメインネームシステム（DNS）キャッシュタイムアウトは、比較的短時間（たとえば 1 分以内）に設定する必要があります。これにより、エンドポイントは、Expressway にアクセスできない場合、すぐに別の Expressway を使用します。

オプション 4 – 静的 IP（4 番目に推奨）

このオプションは、Expressway クラスタにドメインネームシステム（DNS）名がない場合に使用します。

各 SIP エンドポイントで、[SIP 設定（SIP Settings）] を次のように設定します。

- [サーバ検出（Server discovery）] = [手動（Manual）]
- サーバーアドレス = Expressway ピアの IP アドレス

エンドポイントはスタートアップ時に、指定された IP アドレスの Expressway への登録を試行します。この VCS が使用できない場合、エンドポイントは、一定の間隔で試行を続けます。これはエンドポイントが Expressway に登録されるまで繰り返されます。

エンドポイントは、最初に登録した Expressway を再登録および通話に使用します。接続を失った場合でも、再度アクセス可能になるまで、Expressway への登録を試行します。

H.323 エンドポイント

1 つ以上の Expressway クラスタピアにアクセスできなくなった場合に、Expressway のクラスタへのエンドポイントの接続性のレジリエンスを提供するために、オプションが優先設定順に一覧されます。選択するオプションは、使用するエンドポイントがサポートする機能により異なります。

オプション 1 – DNS SRV（推奨）

このオプションを使用するには、各クラスタ ピアで同じウェイトと優先順位を定義する Expressway クラスタの DNS 名で使用できる DNS SRV レコードが必要です。

各 H.323 エンドポイントで、[ゲートキーパー設定（Gatekeeper Settings）] を次のように設定します。

- [検出（Discovery）] = [手動（Manual）]
- IP アドレス = Expressway クライアントのドメインネームシステム（DNS）名

エンドポイントが DNS SRV をサポートする場合、エンドポイントは起動時に DNS SRV 要求を送信して、各クラスタ ピアで同じウェイトと優先順位を定義する DNS SRV レコードを受け取ります。

次に、エンドポイントは、関連するクラスタ ピアへの登録を試行します（優先順位とウェイトが考慮されます）。このピアが使用でいない場合、エンドポイントは、同じ優先順位の別のピ

アへの登録を試行します。同じ優先順位のすべてのピアで登録を試行すると、次に優先順位の低い（大きい数字の）ピアへの登録を試行します。

これは、エンドポイントが Expressway に登録できるまで繰り返されます。Expressway に登録すると、Expressway は、Expressway クラスタピアメンバーのリストを含む H.323 [代替ゲートキーパー（Alternate Gatekeepers）] リストに応答します。

エンドポイントは、最初に登録した Expressway を再登録および通話に使用します。エンドポイントは、その Expressway との接続を失うと、提供されたリストから [代替ゲートキーパー（Alternate Gatekeepers）] を選択します。

DNS SRV キャッシュ タイムアウトは、DNS トラフィックを最小化するために、比較的長時間（たとえば 24 時間）に設定する必要があります。

オプション 2 – DNS ラウンドロビン（2 番目に推奨）

このオプションを使用するには、IP アドレスのラウンドロビンリストを提供する Expressway クラスタの DNS 名で使用できる DNS A レコードが必要です。

各 H.323 エンドポイントで、[ゲートキーパー設定（Gatekeeper Settings）] を次のように設定します。

- [検出（Discovery）] = [手動（Manual）]
- IP アドレス = Expressway クラスタのドメインネームシステム（DNS）名

エンドポイントが DNS SRV をサポートしない場合、エンドポイントは起動時に、DNS A レコードルックアップを実行します。DNS サーバは、各クラスタ ピア メンバーをラウンドロビン リストに定義し、ラウンドロビン DNS をサポートするように設定されます。

エンドポイントは、DNSルックアップにより提供されたアドレスを使用し、関連するクラスタピアへの登録を試行します。そのピアが使用できない場合、エンドポイントは、もう一度DNS探索を実行して、提供される新しいExpresswayピアへの接続を試行します。（DNSサーバは、次のクラスタ ピアの IP アドレスを提供します）。

これは、エンドポイントが Expressway に登録できるまで繰り返されます。Expressway に登録すると、Expressway は、Expressway クラスタピアメンバーのリストを含む H.323 [代替ゲートキーパー（Alternate Gatekeepers）] リストに応答します。

エンドポイントは、最初に登録した Expressway を再登録および通話に使用します。エンドポイントは、接続を失うと、提供されたリストから [代替ゲートキーパー（Alternate Gatekeepers）] を選択します。

DNSキャッシュタイムアウトは、比較的短時間（たとえば1分未満）に設定する必要があります。これにより、エンドポイントは、スタートアップ時に Expressway に到達できない場合、すぐに別の Expressway を使用します。

オプション 3 – 静的 IP（3 番目に推奨）

このオプションは、Expressway クラスタにドメインネームシステム（DNS）名がない場合に使用します。

各 H.323 エンドポイントで、[ゲートキーパー設定（Gatekeeper Settings）] を次のように設定します。

- [検出（Discovery）] = [手動（Manual）]
- IP アドレス = Expressway ピアの IP アドレス

エンドポイントは起動時に、指定された IP アドレスの Expressway への登録を試行します。この VCS が使用できない場合、エンドポイントは、一定の間隔で試行を続けます。

これは、エンドポイントが Expressway に登録できるまで繰り返されます。Expressway に登録すると、Expressway は、Expressway クラスタピアメンバーのリストを含む H.323 [代替ゲートキーパー（Alternate Gatekeepers）] リストに応答します。

エンドポイントは、最初に登録した Expressway を再登録および通話に使用します。エンドポイントは、接続を失うと、提供されたリストから [代替ゲートキーパー（Alternate Gatekeepers）] を選択します。

Cisco TMS に Expressway を追加

Cisco TMS 管理の詳細については、Cisco TelePresence Management Suite（TMS）（TMS 維持および操作ガイドページ）のお使いのバージョンの『Cisco TelePresence Management Suite 管理者ガイド』を参照してください。

Expressway 上

ステップ 1 **[システム（System）]** > **[SNMP]** の順に選択します。

a) **[SNMP モード（SNMP mode）]** を *[v3 と TMS サポート（v3 plus TMS support）]* または *[v2c]* に設定します。

b) **[コミュニティ名（Community name）]** を [パブリック（public）] に設定します。

（SNMP が無効にされていた場合、リスタートが必要なことを示すアラームが表示される場合があります。その場合、**[メンテナンス（Maintenance）]** > **[再起動（Restart）] オプション**の順に選択し、システムを再起動します。）

ステップ 2 **[システム（System）]** > **[外部マネージャ（External manager）]** の順に選択します。

a) **[アドレス（Address）]** を TMS の IP アドレスまたは FQDN に設定します。

b) **[パス（Path）]** を、 `tms/public/external/management/SystemManagementService.asmx` に設定します。

c) **[プロトコル（Protocol）]** が [HTTPS] で、**[証明書検証モード（Certificate verification mode）]** が [オン（On）] の場合、接続が「アクティブ」になる前に、関連する証明書をロードする必要があります。

（**[プロトコル（Protocol）]** が *[HTTP]* で、**[証明書検証モード（Certificate verification mode）]** が *[オフ（Off）]* の場合、証明書をロードする必要はありません）。

ステップ 3 [**Save**] をクリックします。

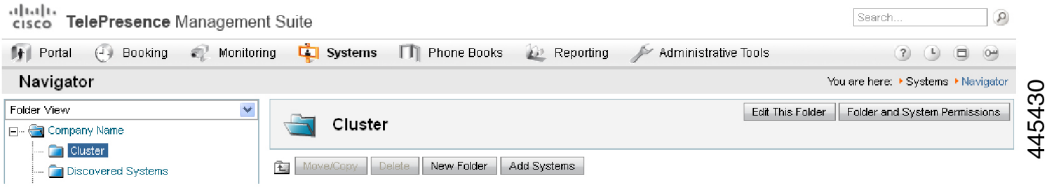
[外部マネージャ（External Manager）] ページの [ステータス（Status）] セクションの [状態（State）] が [アクティブ（Active）] または [初期化中（Initialising）] と表示されています[1]。

1

Cisco TMS 上

ステップ 1 **[システム（Systems）] > [ナビゲータ（Navigator）]** の順に選択します。

ステップ 2 Expressway を含める適切なフォルダを選択（または作成）します（次の例の場合、フォルダの名前は「Cluster」です）。



ステップ 3 [システムの追加（Add Systems）] をクリックします。

ステップ 4 セクション**1**で、**IP アドレスまたはドメインネームシステム（DNS）名**ごとにシステムを指定し、Expressway の IP アドレスまたはドメインネームシステム（DNS）名を入力します。

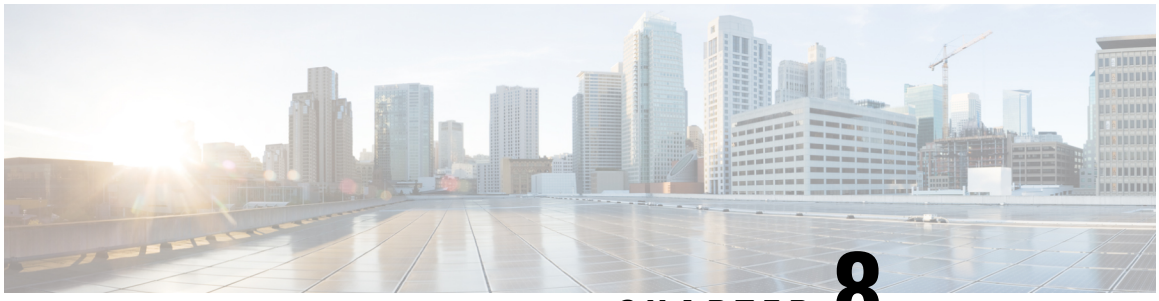
ステップ 5 [Next] をクリックします。

ステップ 6 追加されたシステムの「緑色のチェック」記号を探します。

（注） Expressway を TMS に追加すると、TMS UI に VCS として表示されます。これは既知の問題です。

ステップ 7 必要に応じて、**[システムの追加の完了（Finish Adding Systems）]**、**[警告にかかわらずシステムを登録する（Add System despite warnings）]** または **[システムを追加（Add More Systems）]** をクリックします。

[1] Cisco TMS は、プロトコルを強制的に HTTPS に設定する場合があります。この構成は、**[管理ツール（Administrative Tools）] > [構成（Configuration）] > [ネットワーク設定（Network settings）]** の順に選択すると確認できます。**[TMS サービス（TMS Services）]** セクションで、**[システム上の管理設定の強制（Enforce Management Settings on Systems）]** が *[オン（On）]* に設定され、**[機密保護機能付き専用装置通信（Secure-Only Device Communication）]** セクションで、**[機密保護機能付き専用装置通信（Secure-Only Device Communication）]** が *[オン（On）]* の場合、プロトコルは HTTPS に強制設定されます。



CHAPTER 8

トラブルシューティング

この章では、次の内容について説明します。

バックアップからクラスタを再構築する方法

1. 既存のクラスタ内のすべてのノードを停止します。
2. プライマリに新しい OVA をインストールし、デバイスを起動します。
3. プライマリでバックアップを復元します。プライマリを再起動します。
4. 最初のピアに OVA をインストールし、バックアップから復元します。
5. すべてのピアノードに対して 1 つずつ手順 5 を繰り返します。
6. プライマリノードを再起動します。

シーケンスの再起動

クラスタを形成、接続、アップグレード、または変更した場合は、ピアの再起動が必要かどうかを確認する必要があります。ピア固有の構成変更をした場合は、1 つのピアのみを再起動する必要があります。

クラスタ構成を使用している場合、複数のピアを再起動する必要がある場合があります。この場合、常に次の順序で再起動する必要があります。

1. プライマリピアを再起動し、Web インターフェイス経由でアクセスできるようになるまで待機します。

2. プライマリのクラスタ複製ステータスとすべてのピアのステータスを確認します。数分待って、ピアの Web インターフェイスをときどき更新します。
3. 必要に応じて、一度に 1 つずつ他のピアを再起動します。毎回、アクセス可能になり数分待ってから、複製ステータスを確認します。

レプリケーションステータスの確認

クラスタリングの変更を行った後、Expressway ピアが成功ステータスを報告するまでに約 5 分かかる場合があります。

1. 各ピアで、**[システム（System）]** > **[クラスタリング（Clustering）]** の順に選択し、クラスタデータベースのステータスが [アクティブ（Active）] とレポートされていることを確認します。

   失敗ステータスがある場合は、最初にブラウザを更新します。ステータスが [アクティブ（Active）] でない場合は、アラームを確認します。

Cisco TMS での強制更新

Cisco TMS を使用している場合は、次のように強制的に更新することで、Cisco TMS ですべてのクラスタが正しく設定されていることを確認します。

ステップ 1 Cisco TMS で、**[システム（System）]** > **[ナビゲータ（Navigator）]** の順に選択します。
ステップ 2 Expressway の名前を見つけてクリックします。
ステップ 3 [設定（Settings）] タブを選択します。
ステップ 4 [強制的に更新（Force Refresh）] をクリックします。
ステップ 5 クラスタ内のすべての Expressway ピア（プライマリ Expressway を含む）に対して繰り返します。

Expressway アラームおよび警告

クラスタ名が構成されていません：FindMeまたはクラスタリングが使用中の場合は、クラスタ名を定義する必要があります

同じクラスタ名が、クラスタの各 Expressway で構成されていることを確認します。

クラスタ名は、たとえば、「「cluster1.example.com」」など、この Expressway クラスタに対応する SRV レコードで使用されるルーティング可能な完全修飾ドメイン名にする必要があります（クラスタ名と DNS SRV レコード （61 ページ） を参照）。

クラスタ複製エラー：（詳細）構成を手動で同期する必要があります。

次の場合もあります。

- 「クラスタ複製エラー：構成を手動で同期する必要があります。」
- 「クラスタ複製エラー：構成プライマリ ID が一貫していあせん。構成を手動で同期する必要があります」
- 「クラスタ複製エラー：」このピアの構成がプライマリ構成と競合しています。構成を手動で同期する必要があります

下位 Expressway がアラームを出した場合、「クラスタ複製エラー ー<details>構成の同期」

その下位 Expressway で、次の手順を実行します。

1. admin として SSH または他の CLI インターフェイスでログインします。
2. コマンドプロンプトタイプ：`xcommand ForceConfigUpdate`

   これにより、下位 Expressway 構成が削除され、プライマリ Expressway から構成を強制更新します。

⚠

注意 このコマンドは、プライマリ Expressway の構成が正常な状態である場合のみ使用します。このコマンドを実行する前にバックアップを取ることが推奨されます。

クラスタ複製エラー：（詳細）再起動ノード

次の場合もあります。

“クラスタ複製エラー：プライマリまたはこの下位のピアの構成ファイルが見つかりません。ノードを再起動してください”

ForceConfigUpdate 後もクラスタ複製エラーが解決しない

X8.11 では、クラスタピアごとに一意の暗号キーが導入されました。また、一部のアップグレードの場合、たとえば、ピアが誤った順序でアップグレードされた場合、下位ピアがプライマリと同期しないことがあります。これら 2 つの問題は相互に混在し、ピアがプライマリから構成を復号化できない状態になる可能性があります。

この症状は、下位ピアで `xcommand forceconfigupdate` を試行した後もクラスタ複製アラームが持続することです。これは、プライマリピアで X8.11 にアップグレードした直後である場合があります。

常にプライマリを最初にアップグレードすることで問題を回避できますが、この永続的なエラーが発生する場合は、次のように解決できます。

1. プライマリピアにサインインし、良好な状態であることを確認します。
2. クラスタリング構成で、このピアがプライマリであることが示されていることを確認します。
3. 最初にアップグレードに使用したものと同じパッケージを使用して、プライマリを再度アップグレードします。

プライマリピアがアップグレードされ、リブートされると、複製アラームはクリアされます。これは通常、再起動後 10 分以内に発生しますが、再起動後は最大 20 分かかる場合があります。

クラスタ複製エラー：NTP サーバーに到達できません

[システム（System）] > **[時間（Time）]** ページで Expressway でアクセス可能な NTP サーバーを構成します。

クラスタ複製エラー：ローカルExpresswayがピアのリストにありません

プライマリ Expressway でこの Expressway のピアのリストを確認および修正して、他のすべての Expressway ピアをコピーします（**[システム（System）]**>**[クラスタリング（Clustering）]**）。

クラスタ複製エラー：アップグレード中なので、構成の自動複製が一時的に無効です

アップグレードが完了するまで待ちます。

無効なクラスタリング構成：H.323モードをオンにする必要がありますー クラスタリングは、ピア間で H.323 通信を使用します。

H.323 モードがオンになっていることを確認します（**[構成（Configuration）]** > **[プロトコル（Protocols）]** > **[H.323]** の順に選択して確認）。

Expresswayデータベース障害：シスコサポート担当者に連絡してください

サポート担当者は以下のステップを通じてサポートします。

1. システムのスナップショットを作成し、サポート担当者に提供します。
2. ライブピアをクラスタから永久削除 （33 ページ） を使用して、クラスタから Expressway を削除します。

3. その Expressway で以前に作成したバックアップを復元して、その Expressway データベースをリストアします。
4. クラスタにピアを追加 （20 ページ） を使用して、Expressway をクラスタに再追加します。

Cisco TMS 警告

Cisco TMS クラスタ診断

Cisco TMS クラスタが診断で、Expressway ピアの構成が異なることが報告された場合、各 Expressway の `https://<ip address>/alternatesconfiguration.xml` 出力を比較します。

これらの違いを手動で確認するには、Unix/Linux システムで、次のコマンドを実行します。

```
wget --user=admin --password=<password> --no-check-certificate https://<IP or FQDN of Expressway>/alternatesconfiguration.xml
```

各 Expressway ピアの場合、diff を使用して相違を確認します。

Conference Factory テンプレートが複製されない

これは意図した結果です。Conference Factory %% 値は、クラスタ ピア間で共有されません。Conference Factory アプリケーション設定は、クラスタで複製されません。

「他の Expressway アプリケーションでのクラスタリングの影響 （69 ページ）」を参照してください。

Expressway の外部マネージャプロトコルを HTTPS にセットしたままにする

Cisco TMS は、接続システムで特定の管理設定に強制構成できます。これには、Expressway がフィードバックに HTTPS を使用することを確実にすることが含まれます。有効な場合、Cisco TMS（Cisco TMS で定義されている期間）は、Expressway の **[システム（System）] > [外部マネージャプロトコル（External Manager Protocol）]** を *[HTTPS]* に再構成します。

Expressway が Cisco TMS にフィードバックを提供するために HTTPS を使用する必要がある場合は、Cisco TMS に Expressway を追加 （48 ページ） を参照して、証明書の設定方法を確認してください。

Cisco TMS は、次の場合に Expressway で HTTPS を強制します。

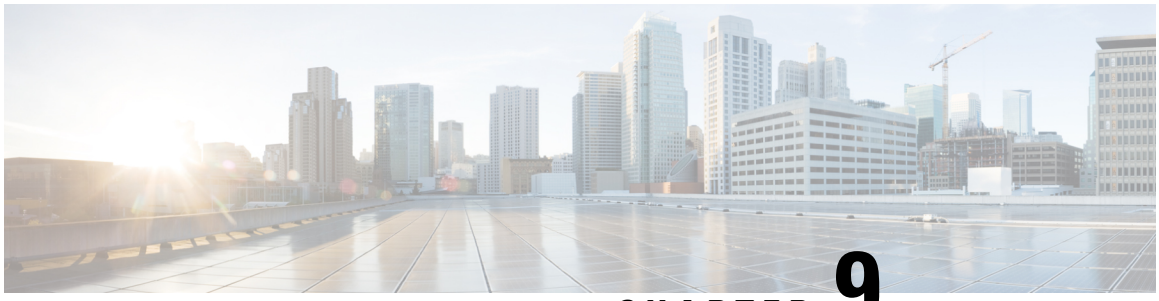
- **[TMS サービス（TMS Services）] > [システム上の管理設定の強制（Enforce Management Settings on Systems）]** = オン（**[管理ツール（Administrative Tools）] > [構成（Configuration）] > [ネットワーク設定（Network Settings）]**）

  および

- **[機密保護機能付き専用装置通信（Secure-Only Device Communication）]** > **[機密保護機能付き専用装置通信（Secure-Only Device Communication）]** = オン (**[管理ツール（Administrative Tools）]** > **[構成（Configuration）]** > **[ネットワーク設定（Network Settings）]**)

Cisco TMS が管理設定を強制設定する必要が無い場合は、**[システム上の管理設定の強制（Enforce Management Settings on Systems）]** を *[オフ（Off）]* に設定します。

Expressway が HTTP（HTTP で十分な場合）を使用して、フィードバックを提供する必要がない場合は、**[機密保護機能付き専用装置通信（Secure-Only Device Communication）]** を *[オフ（Off）]* に設定します。



CHAPTER 9

参照先

この章では、次の内容について説明します。

ピア固有のアイテム

設定のほとんどの項目は、プライマリ ピアを介してクラスタ内のすべてのピアに適用されます。ただし、次の項目（Web インターフェイスで、†でマークされている）は各クラスタ ピアで個別に指定する必要があります。

（注） プライマリピア以外のすべてのピアに適用された構成データは変更しないでください。変更してもマスターから上書きされるか、プライマリの複製に失敗する場合があります。

クラスタ構成（[システム（System）] > [クラスタリング（Clustering）]）

クラスタを構成する**ピア N アドレス**のリスト（ピアそれ自体のアドレスを含む）は各ピアで指定される必要があり、各ピアで一致する必要があります。

各ピアに**[クラスタ名（Cluster name）]**、**[構成プライマリ（Configuration primary）]**、および**[クラスタ IP バージョン（Cluster IP version）]**を指定し、すべてのピアでこれらの項目が一致する必要があります。

（注） クラスタアドレスマッピングを有効にする必要がある場合は、最初にクラスタを IP アドレスで形成することをお勧めします。その後は、1 つのピアにマッピングを追加するだけで済みます。

イーサネット速度（[システム（System）] > [ネットワーク インターフェイス（Network interfaces）] > [イーサネット（Ethernet）]）

イーサネット速度は、各ピアに固有です。各ピアでは、イーサネットスイッチに接続するために多少異なる要件がある場合があります。

IP 構成（[システム（System）]>[ネットワーク インターフェイス（Network interfaces）]>[IP]）

LAN の設定は、各ピアで固有です。

- **IPv4 アドレス**、**IPv6 アドレス**、またはこの両方であるかにかかわらず、ピアごとに一意の IP アドレスが必要です。
- **IP ゲートウェイ**の設定はピアに固有です。各ピアで異なるゲートウェイを使用できます。

各ピアが同じプロトコルをサポートする必要があるので、IP プロトコルがすべてのピアに適用されることに注意してください。

IP 静的ルート（[システム（System）]>[ネットワーク インターフェイス（Network interfaces）]> [静的ルート（Static routes）]）

追加するスタティックルートはピアに固有なので、必要に応じて、異なるルートを異なるピアで作成できます。クラスタ内のすべてのピアが同じスタティックルートを使用できるようにする場合は、各ピアでルートを作成する必要があります。

システム名（[システム（System）] > [管理（Administration）]）

システム名はクラスタ内のピアごとに異なっている必要があります。

DNS サーバーおよび DNS ホスト名（[システム（System）] > [DNS]）

DNS サーバは、各ピアに固有です。各ピアで異なる DNS サーバのセットを使用できます。

システム ホスト名と**ドメイン名**は各ピアに固有です。

NTP サーバーおよびタイムゾーン（[システム（System）] > [時間（Time）]）

NTP サーバは各ピアに固有です。各ピアで、1 つ以上の異なる NTP サーバを使用できます。

タイム ゾーンは各ピアに固有です。各ピアで異なる現地時間を設定できます。

SNMP（[システム（System）] > [SNMP]）

SNMP 設定は、各ピアに固有です。また、各ピアで異なることができます。

ロギング（[メンテナンス（Maintenance）] > [ロギング（Logging）]）

各ピアのイベント ログおよびコンフィグレーション ログは、特定の Expressway のアクティビティのみを報告します。ログ レベルとリモート syslog サーバのリストは各ピアに固有です。すべてのピアのログを送信できるリモート syslog サーバを設定することを推奨します。これにより、クラスタ内のすべてのピア間でアクティビティの全体像を把握できます。

セキュリティ証明書（[メンテナンス（Maintenance）] > [セキュリティ（Security）]）

Expressway が使用する信頼できる CA 証明書とサーバ証明書および証明書失効リスト（CRL）は、ピアごとに個別にアップロードする必要があります。

管理アクセス（[システム（System）] > [管理（Administration）]）

次のシステム管理アクセス設定は各ピアに固有です。

- シリアル ポート/コンソール
- SSH サービス
- Web インターフェイス（HTTPS 経由）
- HTTP リクエストを HTTPS にリダイレクト
- 自動保護サービス

オプションキー（[メンテナンス（Maintenance）] > [オプションキー（Option keys）]）

機能を制御するオプション キーは、適用されるピアに固有です。ライセンスを制御するオプション キーは、クラスタ全体で使用するようにプールされています。

各ピアでは、同一セットの機能オプション キーがインストールされている必要があります。このため、クラスタ内の各ピアにキーを購入する必要があります。

ライセンス オプション キーは、クラスタ内の 1 つ以上のピアに適用できます。インストール済みライセンスの合計がクラスタ全体で使用できます。ライセンス プーリング動作には次のオプション キーが含まれます。

- Expressway：リッチ メディア セッション
- Expressway：TelePresence ルーム システム
- Expressway：デスクトップ システム
- VCS：トラバーサル コール
- VCS：非トラバーサル コール

（注） クラスタ内でライセンスが使用できても、必要なライセンスを有効にするキーがないことを示すアラームがピアに表示される場合があります。必要なライセンスがインストールされたピアが 1 つだけで、サービスを中断していない限り、このカテゴリのアラームは確認して、無視できます。

Active Directory サービス（[構成（Configuration）] > [認証（Authentication）] > [デバイス（Devices）] > [Active Directory サービス（Active Directory Service）]）

デバイス認証のために Active Directory サービスへの接続を設定する場合、[NetBIOS マシン名（上書き）（NetBIOS machine name (override)）] とドメイン管理者の [ユーザ名（Username）] および [パスワード（Password）] は各ピアに固有です。

Conference Factory テンプレート（[アプリケーション（Applications）] > [Conference Factory]）

Conference Factory アプリケーションで会議サーバにコールをルーティングするために使用するテンプレートは、クラスタ内の各ピアに固有です。

クラスタ内 TLS ポートを保護するためのサンプル ファイアウォール ルール

サービス妨害攻撃からクラスタピアを保護するには、Expressway の組み込みファイアウォールルールを使用して、クラスタリングポートへのすべての TCP アクセスをフィルタリングすることをお勧めします。

各ピアで、次の手順を実行します。

1. **[システム（System）] > [保護（Protection）] > [ファイアウォールルール（Firewall rules）] > [構成（Configuration）]** の順に選択します。
2. 適切な（IPv4 または IPv6）範囲内のすべての IP アドレスに、ポート 4371 および 4372 への TCP 接続をドロップするルールを追加します。
3. 他のピアの IP アドレスごとに 1 つずつ、優先順位の低いルールを追加し、それらのポートへの TCP 接続を許可します。

   （小さい番号のルールは、大きい番号のルールの前に実装されます）。
4. ファイアウォールルールをアクティブにします。

図 *1*：特定のピアがこのピアのクラスタリングポートに接続できるようにするカスタムルールの作成

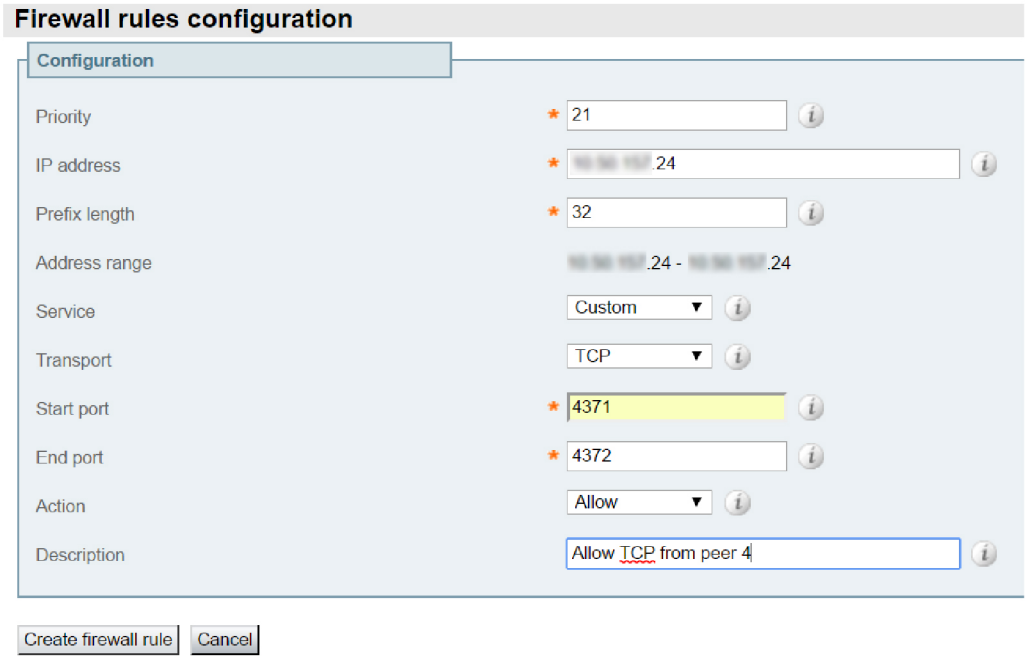
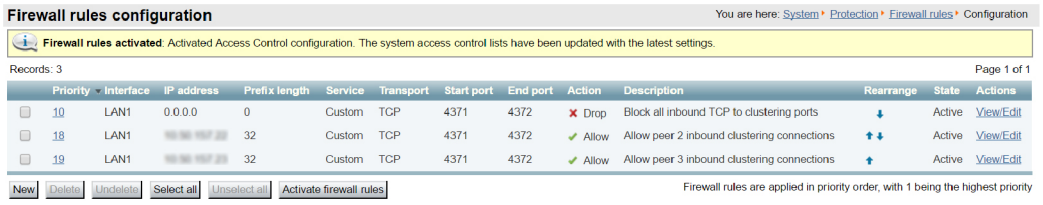


図 *2*：推奨される優先順位を示すルールのリストの例



クラスタ名と DNS SRV レコード

DNS SRV を使用してドメインを IP アドレスに変換する場合、次のような多くの利点があります。

- ルックアップの構造に、サービスタイプとプロトコルおよびドメインが含まれます。これにより、共通するドメインを使用して、異なるマシンでホストされる複数の異なるサービスを参照できます（たとえば、HTTP、SIP、H.323）。
- DNS SRV 応答に優先順位とウェイト値が含まれます。これにより、サーバのプライマリ、セカンダリ、ターシャリなどのグループを指定できます。また、各優先順位グループ内で、ウェイトは、各サーバを使用するアクセスの比率を定義します。

- DNS SRV の応答に複数のサーバーの優先順位とウェイトに関する詳細が含まれているため、受信デバイスは、DNS サーバーに繰り返し問いクエリする必要がなく、稼働中のサーバー（一部のサーバーがアクセスできない場合）の検索に単一のルックアップを使用できます。（これは、最初のサーバーがアクセスできないことが判明している場合に、DNS サーバーへの繰り返しルックアップを必要とするラウンドロビン DNS を使用する場合と対照的です）。

次に、DNS SRV クエリの通常のフォーマットを示します。

- _service._protocol.<fully.qualified.domain>

DNS SRV 応答は、次のフォーマットのレコードのセットです。

- _service._ protocol.<fully.qualified.domain>。TTL Class SRV Priority Weight Port Target

  ここで、Target は、宛先を定義する A レコードです。

DNS SRV の詳細については、『Expressway 管理者ガイド』「RFC 2782」を参照してください。

モバイルおよびリモートアクセス用の DNS SRV 構成

ここでは、MRA のパブリック（外部）とローカル（内部）ドメインネームシステム（DNS）の要件について説明します。詳細については、[Jabber インストールおよびアップグレードガイド（Jabber Install and Upgrade Guides）] ページの『Cisco Jabber 計画ガイド』を参照してください。

重要 **バージョン X8.8 以降では、すべての Expressway-E システムに対して順方向および逆方向の DNS エントリを作成する必要があります。これにより、それらへの TLS 接続を行うシステムが FQDN を解決し、証明書を検証できます。**

パブリック ドメインネームシステム（DNS）（外部ドメイン）

エンドポイントがモバイルおよびリモートアクセスに使用する Expressway-E を検出できるようにするため、パブリックの外部ドメインネームシステム（DNS）は、*_collab-edge._tls.<domain>* SRV レコードで設定する必要があります。 また、一般的な展開（特に MRA 用ではない）の SIP サービスレコードも必要です。たとえば、2 つの Expressway- E システムのクラスタの場合は、次のようになります。

表 *2:*

ドメイン	サービス	プロトコル	プライオリティ	ウェイト	ポート	ターゲットホスト
example.com	collab-edge	tls	10	10	8443	expe1.example.com
example.com	collab-edge	tls	10	10	8443	expe2.example.com
example.com	sips	tcp	10	10	5061	vcse1.example.com

ドメイン	サービス	プロトコル	プライオリティ	ウェイト	ポート	ターゲットホスト
example.com	sips	tcp	10	10	5061	vcse2example.com

ローカル ドメインネームシステム（DNS）（内部ドメイン）

ローカルの内部ドメインネームシステム（DNS）を *_cisco-uds._tcp.<domain>* SRV レコードで構成することが推奨されていても、これは、X12.5 以降で要件ではなくなります。レコードの例：

表 *3：*

ドメイン	サービス	プロトコル	プライオリティ	ウェイト	ポート	ターゲットホスト
example.com	cisco-uds	tcp	10	10	8443	cucm.example.com
example.com	cisco-uds	tcp	10	10	8443	cucm2.example.com

MRA を使用するすべての Unified Communications ノードに対する正引きおよび reverse ルックアップの両方に内部ドメインネームシステム（DNS）を作成します。これにより、IPアドレスまたはホスト名がFQDNの代わりに使用されている場合に、のノードを検索することができます。

cisco-uds SRV レコードが内部ネットワーク外で解決できないことを確認します。解決できてしまうと、Jabber クライアントが Expressway-E 経由で MRA を開始しません。

ビデオ会議の DNS SRV 設定

次に、Expressway で使用される sip（RFC 3263）および H.323 の DNS SRV クエリのフォーマットを示します。

- _sips._tcp.<fully.qualified.domain>
- _sip._tcp.<fully.qualified.domain>
- _sip._udp.<fully.qualified.domain> ：ビデオ コールにはお勧めしません。オーディオ専用コールのみに使用します。
- _h323ls._udp.<fully.qualified.domain>：LRQ などの UDP の場所（RAS）シグナリングに使用します。
- _h323cs._tcp.<fully.qualified.domain> ：H.323 コール シグナリングに使用します。

次に、エンドポイントにより通常使用される sip（RFC 3263）および H.323 の DNS SRV クエリのフォーマットを示します。

- _sips._tcp.<fully.qualified.domain>
- _sip._tcp.<fully.qualified.domain>

- _sip._udp.<fully.qualified.domain> ：ビデオ コールにはお勧めしません。オーディオ専用コールのみに使用します。
- _h323ls._udp.<fully.qualified.domain>：LRQ などの UDP の場所（RAS）シグナリングに使用します。
- _h323cs._tcp.<fully.qualified.domain> ：H.323 コール シグナリングに使用します。
- _h323rs._udp.<fully.qualified.domain> ：H.323 登録に使用します。

UDPはビデオシグナリング向けに推奨されたトランスポートメディアではありません。ビデオシステムのSIPメッセージングはデータグラムベース（ストリームベースではなく）のトランスポートを信頼できる形で続行するには大きすぎます。

Expressway **クラスタ名（[システム（System）] > [クラスタリング（Clustering）]** ページで構成）は FQDN である必要があります。ドメイン部分は、その Expressway クラスタを指す SRV レコードに使用されるドメインです。

例

example.com の Expressway-E クラスタ の 2 ピアの DNS SRV レコード

定義：

- Expressway-E ピア 1 の FQDN：expe1.example.com
- Expressway-E ピア 2 の FQDN：expe2.example.com
- Expressway-E クラスタの FQDN：cluster.example.com

```
_sips._tcp.example.com. 86400 IN SRV 1 1 5061 expe1.example.com.
_sips._tcp.example.com. 86400 IN SRV 1 1 5061 expe2.example.com.

_sip._tcp.example.com. 86400 IN SRV 1 1 5060 expe1.example.com.
_sip._tcp.example.com. 86400 IN SRV 1 1 5060 expe2.example.com.

_h323ls._udp.example.com. 86400 IN SRV 1 1 1719 expe1.example.com.
_h323ls._udp.example.com. 86400 IN SRV 1 1 1719 expe2.example.com.

_h323cs._tcp.example.com. 86400 IN SRV 1 1 1720 expe1.example.com.
_h323cs._tcp.example.com. 86400 IN SRV 1 1 1720 expe2.example.com.

_h323rs._udp.example.com. 86400 IN SRV 1 1 1719 expe1.example.com.
_h323rs._udp.example.com. 86400 IN SRV 1 1 1719 expe2.example.com.
```

（注）
- 優先順位はすべて同じです。1 つのプライマリクラスタから別のクラスタ（セカンダリ）へのフェールオーバーを許可する異なるクラスタが設定されている場合は、異なる優先順位のみを使用します。この場合、プライマリクラスタピアに1つの値が必要であり、その他（セカンダリ）クラウドピアにはより大きな値が必要になります。
- 各ピアが均等に使用されるように、ウェイトは同じである必要があります。

DNS SRV 設定の確認

Expressway からの DNS SRV 接続の確認

1. **[メンテナンス（Maintenance）]** > **ツール（Tools）]** > **[ネットワークユーティリティ（Network utilities）]** > **[接続テスト（Connectivity Test）]** に移動します。
2. クエリする **[サービスレコードドメイン（Service Record Domain）]** を入力します（例：`call.ciscospark.com`）。
3. テストする [サービスレコードプロトコル（Service Record Protocols）] を入力します（例：`_sips._tcp`）。

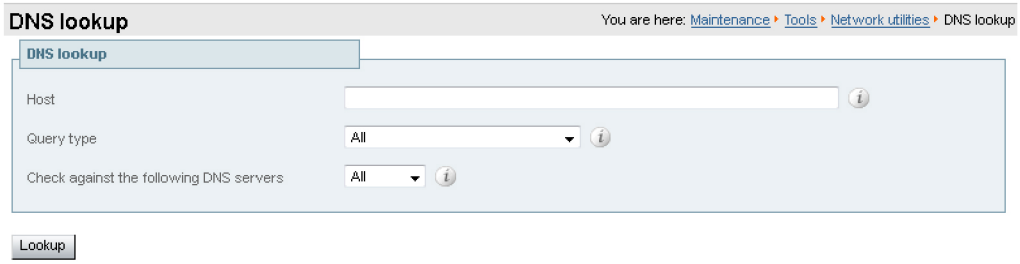
   複数のプロトコルを指定する場合は、各プロトコルをカンマで区切ります（例：`_sip._tcp`, `_sips._tcp`）。
4. [実行（Run）] をクリックします。

Expressway は、サービス、プロトコル、ドメインの組み合わせで構成される SRV レコードに対してドメインネームシステム（DNS）にクエリします。例：`_sip._tcp.call.ciscospark.com` および `_sips._tcp.call.ciscospark.com`。

デフォルトでは、システムは、すべてのシステムデフォルト DNS サーバー（**[システム（System）]** > **[DNS]**）にクエリを送信します。

Expressway で DNS 探索ツールを使用する

1. **[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[ネットワークユーティリティ（Network utilities）]** > **[DNS 探索（DNS lookup）]** の順に選択します。
2. **[ホスト（Host）]** フィールドに SRV のパスを入力します。
3. [Lookup] をクリックします。



nslookup

```
nslookup -query=SRV _sip._tcp.example.com
```

dig

```
dig _sip._tcp.example.com SRV
```

```
; <<>> DiG 9.4.1 <<>> _sip._tcp.example.com SRV
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44952
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 4

;; QUESTION SECTION:
;_sip._tcp.example.com.          IN      SRV

;; ANSWER SECTION:
_sip._tcp.example.com. 1183     IN      SRV 1 0 5060 expe1.example.com.
_sip._tcp.example.com. 1183     IN      SRV 1 0 5060 expe2.example.com.

;; AUTHORITY SECTION:
example.com.      87450      IN      NS      ns1.mydyndns.org.
example.com.      87450      IN      NS      ns2.mydyndns.org.

;; ADDITIONAL SECTION:
expe1.example.com.      1536     IN      A      194.73.59.53
expe2.example.com.      1376     IN      A      194.73.59.54
ns1.mydyndns.org.       75       IN      A      204.13.248.76
ns2.mydyndns.org.      10037     IN      A      204.13.249.76

;; Query time: 0 msec

~ #
```

隔離されたネットワークのクラスタ

（注） この付録の背景情報は有効ですが、説明されている問題と回避策は、X8.9.2 の修正によって無効になりました。この修正により、DNS 探索によって返される IP アドレスを使用する代わりに、ピア FQDN をピア IP アドレスにプライベートにマッピングできます。

X8.8 では、Expressway ピアは TLS を使用して相互に通信します。許可された TLS（証明書が検証されない）と、証明書が検証された強制 TLS のオプションがあります。

後者の場合、各ピアは、ピアの証明書から読み取った共通名（CN）と、場合によってはサブジェクト代替名（SAN）をドメインネームシステム（DNS）検索する必要があります。返された IP アドレスを証明書を提供した IP アドレスと比較し、一致した場合は、接続が認証されます。

隔離されたネットワークでは、ピアは通常、内部 DNS サーバーに到達できません。これは、一方的なインバウンド要求が必要になるためです。デュアル NIC セットアップでは、ピアのプライベート IP アドレスをパブリックドメインネームシステム（DNS）に配置する必要はありません。

この問題は、サーバー証明書で IP アドレスを共通名またはサブジェクト代替名として使用できないことで悪化します。認証局はこれを提唱しておらず、おそらくそのような証明書を発行しません。

Expressway-E ピアにはデュアル NIC があり、静的 NAT はありません。

クラスタピア間で TLS を適用できます。

1. 各ピアのドメインネームシステム（DNS）構成で、パブリック DNS サーバーを入力します。
2. パブリックアドレスを取得する LAN インターフェイスを選択します。
3. 各ピアの FQDN をパブリック IP アドレスに解決するようにパブリックドメインネームシステム（DNS）を構成します。
4. すべてのピア証明書の CN に同じクラスタ FQDN を入力し、各ピア証明書の SAN にそのピアの FQDN を入力します。
5. クラスタリング構成ページでクラスタ FQDN とピア FQDN を入力し、**[TLS 検証モード（TLS verification mode）]** を [強制（Enforce）] に設定します。

ピアは、証明書に示されているように、パブリックドメインネームシステム（DNS）を使用して互いの ID を確認します。

Expressway-E ピアにはデュアル NIC があり、静的 NAT が有効になっています。

隔離されたネットワーク内のプライベート IP アドレスに加えて、いずれかの NIC にプライベートアドレスに変換されるパブリック IP アドレスを指定できます。この場合、FQDN を使用してクラスタを形成することはできません。

これは、各ピアの FQDN のパブリック DNS レコードは変換された（パブリック）IP アドレスと一致しますが、証明書を交換するときにピアが互いのプライベートアドレスを参照するためです。IP アドレスが一致しないと、TLS 接続が確立されず、クラスタが形成されません。

クラスタを形成するには、次の手順を実行します。

1. 各ピアのドメインネームシステム（DNS）構成でパブリック DNS サーバーを入力します。
2. 各ピアのどの LAN インターフェイスで静的 NAT を有効にするかを選択します。
3. クラスタリング構成ページで他の LAN インターフェイスのプライベート IP アドレスを入力し、TLS モードを [許可（Permissive）] に設定します。

ピアはプライベート IP アドレスを使用してクラスタを形成しますが、証明書の内容を DNS レコードと照合しません。

NAPTR レコード

NAPTR レコードは、通常、電子メール、SIP、H.323 など、宛先 URI へのさまざまな接続方式を指定するときに使用されます。また、たとえば、SIP TCP または SIP UDP より SIP TLS を優先するなど、接続タイプに使用する優先順位を指定するときにも使用されます。

NAPTR レコードは、電話番号をダイヤル可能 URI に変換するときに、ENUM で使用されます（列挙型の詳細については、『列挙型ダイヤリングに関する Expressway 導入ガイド』を参照してください）。

NAPTR レコードフォーマット

例：example.com への SIP アクセス、および 557120、557121、557122 の列挙型ルックアップ

$ORIGIN example.com.

```
IN    NAPTR    10    100    "s"    "SIPS+D2T"    ""    _sips._tcp.example.com.
IN    NAPTR    12    100    "s"    "SIP+D2T"     ""    _sip._tcp.example.com.
IN    NAPTR    14    100    "s"    "SIP+D2U"     ""    _sip._udp.example.com.
```

$ORIGIN www.example.com.

```
IN    NAPTR    10    100    "s"    "http+I2R"    ""    _http._tcp.example.com.
IN    NAPTR    10    100    "s"    "ftp+I2R"     ""    _ftp._tcp.example.com.
```

$ORIGIN 0.2.1.7.5.5.enum.lookup.com.

```
IN    NAPTR    10    100    "u"    "E2U+sip"     "!^.*$!john.smith@tandberg.com!"
    .
IN    NAPTR    12    100    "u"    "E2U+h323"    "!^.*$!john.smith@tandberg.com!"
    .
IN    NAPTR    10    100    "u"    "mailto+E2U"  "!^.*$!mailto:john.smith@tandberg.com!"
   .
```

$ORIGIN 1.2.1.7.5.5.enum.lookup.com.

```
IN    NAPTR    10    100    "u"    "E2U+sip"    "!^.*$!mary.jones@tandberg.com!"    .
```

$ORIGIN 2.2.1.7.5.5.enum.lookup.com.

```
IN    NAPTR    10    100    "u"    "E2U+h323" "!^.*$!peter.archibald@myco.com!"    .
```

```
IN = Internet routing NAPTR = record type
        10 = order value (use lowest order value first)
                100 = preference value if multiple entries have the same order value
                        "u" = the result is a routable URI
                        "s" = the result is a DNS SRV record
                        "a" = the result is an 'A'or 'AAAA' record
                                "E2U+sip" to make SIP call
                                "E2U+h323" to make h.323 call
                                        Regular expression:
                                        ! = delimiter
                                        "" = no expression used
                                        … usual Regex expressions can be used
                                                Replace field; . = not used
```

ENUM NAPTR レコードの検索

```
dig 4.3.7.8.enum4.example.com. NAPTR
```

```
; <<>> ;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38428
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;4.3.7.8.enum4.example.com. IN NAPTR

;; ANSWER SECTION:
4.3.7.8.enum4.example.com. 60 IN NAPTR 10 100 "u" "E2U+sip" "!^.*$!bob@example.com!" .
4.3.7.8.enum4.example.com. 60 IN NAPTR 10 100 "u" "E2U+h323" "!^.*$!bob@example.com!" .


;; AUTHORITY SECTION:
enum4.example.com. 60 IN NS int-server1.example.com.
```

```
;; ADDITIONAL SECTION:
int-server1.example.com. 3600 IN A 10.44.9.144
int-server1.example.com. 3600 IN AAAA 3ffe:80ee:3706::9:144

;; Query time: 0 msec
```

Domain NAPTR レコードの検索

例：パブリック（外部）ネットワークにあることをエンドポイントが検出できるようにする NAPTR レコードフラグ「s」は、「se」に拡張され、「外部」であることを示します

```
~ # dig -t NAPTR example.com
; <<>> DiG 9.4.1 <<>> -t NAPTR example.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1895
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 6, ADDITIONAL: 4

;; QUESTION SECTION:
;example.com. IN NAPTR

;; ANSWER SECTION:
example.com. 2 IN NAPTR 50 50 "se" "SIPS+D2T" "" _sips._tcp.example.com.
example.com. 2 IN NAPTR 90 50 "se" "SIP+D2T" "" _sip._tcp.example.com.
example.com. 2 IN NAPTR 100 50 "se" "SIP+D2U" "" _sip._udp.example.com.

;; AUTHORITY SECTION:
example.com. 320069 IN NS nserver2.example.com.
example.com. 320069 IN NS nserver.euro.example.com.
example.com. 320069 IN NS nserver.example.com.
example.com. 320069 IN NS nserver3.example.com.
example.com. 320069 IN NS nserver4.example.com.
example.com. 320069 IN NS nserver.asia.example.com.

;; ADDITIONAL SECTION:
nserver.example.com. 56190 IN A 17.111.10.50
nserver2.example.com. 57247 IN A 17.111.10.59
nserver3.example.com. 57581 IN A 17.22.14.50
nserver4.example.com. 57452 IN A 17.22.14.59

;; Query time: 11 msec
```

他の Expressway アプリケーションでのクラスタリングの影響

Conference Factory（Multiway™）

クラスタで Conference Factory（Multiway）を使用する場合は、次の点に注意してください。

- Conference Factory アプリケーション設定はクラスタ間で複製されません。
- Conference Factory テンプレートは、各 Expressway ピアで異なる必要があります。

Multiway をサポートするようにクラスタを設定するには、次の手順を実行します。

1. 各ピアで**同じ** Conference Factory **エイリアス**を設定します（エイリアスは、Multiway 会議を開始するときにエンドポイントによりコールされます）。

2. 各ピアで**異なる** Conference Factory **テンプレート**を設定します（これにより、各ピアで独自の Multiway 会議 ID が生成されます）。

たとえば、アドホック会議の MCU サービスプレフィックスが 775 の場合、プライマリ Expressway は `775001%%@domain` のテンプレート、ピア 2 は `775002%%@domain` のテンプレート、ピア 3 は `775003%%@domain` のテンプレートを使用する場合があります。Expressway が会議 ID を提供する場合、他の Expressway と共有する可能性がある会議 ID を提供することはできません。

これは、ネットワーク間でも同様です。ネットワークで Conference Factory 機能を提供する複数の Expressway または Expressway クラスタがある場合、各 Expressway およびすべての Expressway は、同じ会議 ID が使用されないように、独自の範囲の値を提供する必要があります。

詳細については、『Cisco TelePresence Multiway 導入ガイド』を参照してください。

Microsoft 製品との相互運用性

Microsoft インフラストラクチャが Expressway クラスタで展開されている場合は、『Expressway および Microsoft インフラストラクチャ導入ガイド』を参照してください。

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。