



Cisco Expressway クラスターの作成およびメンテナンス 展開ガイド (X14.3)

最終更新：2025年7月9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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023-2025 Cisco Systems, Inc. All rights reserved.



目次

Full Cisco Trademarks with Software License ?

第 1 章	このマニュアルについて 1
	対象となる情報 1
	変更履歴 2

第 2 章	クラスタリングの基礎 7
	概要 7
	クラスタリングの利点 7
	容量の増加について 8
	ライセンスについて 8

第 3 章	クラスタリングの要件 9
	Expressway-C と Expressway-E を混在させないでください 9
	プラットフォームとソフトウェアのバージョンが一致 9
	ネットワーク条件が満たされている 10
	基本設定が完了しました 10
	DNS 構成が完了しました 11
	TMS 設定済み (必須の場合) 12
	CE1200 および CE1100 物理アプライアンスが混在するクラスタ 12
	Expressway と Expressway Select によるクラスタ導入の混在 12

第 4 章	クラスタを形成する方法 13
	概要 13

クラスタに参加するための Expressway の準備	14
Expressway ピアの新しいクラスタを作成する	16
次のステップ	20
クラスタにピアを追加する	20
確認	21
次のステップ	22

第 5 章

(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	23
Expressway-E クラスタのクラスタアドレスマッピング	23
クラスタアドレスマッピングが必要か	23
クラスタ アドレス マッピングの仕組み	24
推奨されるマッピングの出所	24
クラスタ アドレス マッピングの構成 (Expressway-E クラスタ)	25
FQDN を使用するようにクラスタを変更する	26
TLS 検証の強制	29
事前準備	29
TLS 検証を強制するプロセス	29
Expressway-E トラバーサルゾーンの使用上の注意	29

第 6 章

クラスタを変更する方法	31
クラスタを変更する前に	32
クラスタからライブピアを（永久に）削除する	33
クラスタから削除する Expressway 上	33
プライマリ Expressway 上	34
残りのすべての下位 Expressway ピア	35
クラスタからデッドピアを（永久に）削除する	35
このピアの設定を消去	36
Expressway クラスタ ピアの復旧	37
クラスタの解除	37
プライマリ ピアの変更	38
ピア アイデンティティの変更	39

	ピアの置き換え	40
	ピアを置き換え、その構成を移行する	41
第 7 章	Expressway クラスタを他のシステムに接続する方法	43
	Expressway クラスタ間の近隣	43
	クラスタと連携するためのエンドポイントの設定	43
	SIP エンドポイント	44
	オプション 1 - SIP アウトバウンド (優先)	44
	オプション 2 - DNS SRV (第 2 選択)	45
	オプション 3 - DNS ラウンドロビン (第 3 選択)	45
	オプション 4 - 静的 IP (最も優先度が低い)	46
	H.323 エンドポイント	46
	オプション 1 - DNS SRV (優先)	46
	オプション 2 - DNS ラウンドロビン (第 2 選択)	47
	オプション 3 - 静的 IP (最も優先度が低い)	47
	Expressway を Cisco TMS に追加する	48
	Expressway 上	48
	Cisco TMS 上	49
第 8 章	トラブルシューティング	51
	シーケンスの再起動	51
	レプリケーション状況の確認	51
	Cisco TMS での強制更新	52
	Expressway のアラームと警告	52
	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されている場合、 クラスタ名を定義する必要があります	52
	クラスタレプリケーションエラー: (詳細) 構成の手動同期が必要です	52
	クラスタレプリケーションエラー: (詳細) ノードを再起動してください	53
	ForceConfigUpdate 後もクラスタ レプリケーションエラーが持続する	53
	クラスタレプリケーションエラー: NTP サーバーに到達できません	54

クラスタレプリケーションエラー: ローカル Expressway がピアのリストに表示されません
54

クラスタレプリケーションエラー: アップグレードが進行中のため、構成の自動レプリケーションは一時的に無効になっています 54

無効なクラスタ構成です: H.323 モードをオンにする必要があります-クラスタリングはピア間の H.323 通信を使用します 54

Expressway データベースエラー: Cisco サポート担当者に連絡してください 54

Cisco TMS 警告 55

Cisco TMS クラスタ診断 55

会議ファクトリ テンプレートが複製されない 55

Expressway の外部マネージャプロトコルが繰り返し HTTPS に設定される 55

第 9 章

参照先 57

ピア固有のアイテム 57

クラスタ内 TLS ポートを保護するためのサンプルのファイアウォールルール 60

クラスタ名および DNS SRV レコード 61

モバイルおよびリモート アクセスの DNS SRV 設定 62

ビデオ会議のための DNS SRV 構成 63

DNS SRV 設定を確認する 65

隔離されたネットワークのクラスタ 66

NAPTR レコード 67

NAPTR レコード形式 67

他の Expressway アプリケーションにおけるクラスタリングの影響 69

会議ファクトリ (Multiway™) 69

Microsoft 製品との相互運用性 70



第 1 章

このマニュアルについて

この章では、次の項目について説明します。

- [対象となる情報](#) (1 ページ)
- [変更履歴](#) (2 ページ)

対象となる情報

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 上の古い VCS ガイドは、各ガイドのタイトルページに指定されている VCS バージョンに対して依然として有効です。

このガイドの内容は次のとおりです。

- [クラスタリングの要件](#)

ピア Expressway をクラスタリングする前に必要なネットワーク環境と最小構成について説明しています。

- [クラスタを形成する方法](#)

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。

- [クラスタを変更する方法](#)

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](#)

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

- [トラブルシューティング](#)

クラスタが期待通りに動作しない場合に役立つガイダンスです。

- 参照先

お使いの環境に関連する可能性のある追加資料。

クラスタ化システムでのライセンスの使用状況と容量の詳細については、Cisco Expressway シリーズの [管理と運用ガイド](#) ページで『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 (Date)	変更内容 (Change)	理由 (Reason)
2025 年 3 月	「トラブルシューティング」の章から「バックアップからクラスタを再構築する方法」のセクションを削除しました。	X14.3 リリースを再公開しました。
2023 年 6 月	X14.3 リリース用に初版発行 「(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 「クラスタ要件」の章の 「Expressway による混合クラスタの展開と Expressway 選択」セクションにメモを追加	X14.3 リリース
2021 年 7 月	X14.0.2 リリースの更新 いくつかの CDET に対処しました	X14.0.2 リリース
2021 年 4 月	X14.0 リリースの最初の公開 「トラブルシューティング」の章に「Expressway のアラームと警告」を追加	X14.0 リリース

日付 (Date)	変更内容 (Change)	理由 (Reason)
2020年6月	<ul style="list-style-type: none"> • X12.6用に更新。また、クラスタライセンスの使用状況と容量のガイドラインを削除。このガイドラインは現在、Expressway 管理者ガイドに含まれています。 • [クラスタリング要件]を更新して、B2B 展開のピアごとに A または AAAA レコードを持つ DNS SRV レコードを明確にすることが推奨されますが、必須ではありません。 	X12.6リリースとドキュメントの修正
2019年3月	クラスタピアを削除すると、デュアルNIC 導入の LAN2 インターフェイスのすべての設定が削除されることを明記。	明確化
2019年2月	X12.5用に更新。 このバージョンから、ガイドは Cisco Expressway シリーズにのみ適用され、Cisco VCSには適用されません。	X12.5 リリース
2019年2月	クラスタアドレスマッピングのセクションが編集されました。ソフトウェアバージョンが X8.11.4 メンテナンス リリースに更新されました。テキストへのその他の軽微な強化。	ドキュメントの欠陥、X8.11.4 リリース
2018年9月	Webex および Spark プラットフォームのリブランディング、CE1200 アプライアンス、X8.11.1 メンテナンス リリースのために更新されました。	X8.11.1 リリース

日付 (Date)	変更内容 (Change)	理由 (Reason)
2018年8月	「「クラスタ名およびDNS SRV レコード」」セクションのテキストと例を修正しました。	修正
2018年7月	X8.11用に更新。	X8.11 リリース
2017年11月	「前提条件」セクションのラウンドトリップ遅延と最大ホップ距離を更新。	アップデート
2017年10月	クラスタのアップグレードの順番に関するアドバイスを強化しました。	明確化
2017年8月	すべてのクラスタ ピアは同じドメインで設定する必要があるというメモを追加しました。	省略
2017年7月	X8.10用に更新。	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しました。	X8.9.2 リリース
2016年12月	TLSに関連して、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しました。	X8.9 リリース
2016年6月	クラスタ通信で TLS を使用するようになりました。 Expressway に登録、FindMe、TMSPE サポートを導入。	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。ピアを置き換えるための新しい手順。	
2015年4月	X8.5以降用にメニューパスを変更。X8.5.2で再公開されました。	
2014年12月	X8.5用に更新。	

日付 (Date)	変更内容 (Change)	理由 (Reason)
2014年6月	X8.2用に再発行。	
2014年4月	Expressway X8.1.1用に更新。 <ul style="list-style-type: none">• Expresswayの新しい「クラスタのアップグレード」セクション• 新しい「Expresswayピアの交換」セクション• 「IPポートとプロトコル」付録の更新	
2013年12月	このドキュメントのExpresswayバージョンの最初のリリースです。古いVCSバージョンについては、「 VCS設定ガイド 」ページを参照してください。	



第 2 章

クラスタリングの基礎

この章では、次の項目について説明します。

- [概要 \(7 ページ\)](#)

概要

Expressway は、最大 6 つの Expressway のクラスタの一部にすることができます。クラスタ内の各 Expressway は、そのクラスタ内の他のすべての Expressway のピアです。クラスタを作成するとき、1 つのピアをプライマリとして指定します。プライマリから、その構成が他のピアに複製されます。

クラスタ内のすべての Expressway ピアは、同じルーティング機能を持つ必要があります — いずれかの Expressway が通話を宛先にルーティングできる場合、そのクラスタ内のすべての Expressway ピアは、通話を宛先にルーティングできると想定されます。ルーティングが異なる Expressway ピアの場合、別々の 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 は、容量と復元力の両方にメリットがあります。

- **容量。** クラスタリングは、単一の Expressway と比較して、Expressway 展開の容量を最大で 4 倍に増やすことができます。
- **復元力。** クラスタリングは Expressway がメンテナンスモードの間、あるいはネットワークや停電によりアクセス不能になった場合に冗長性を提供します。クラスタ内の Expressway ピアは、帯域幅の使用状況に加えて、ルーティング、ゾーン、その他の構成を共有します。エンドポイントはクラスタ内の任意のピアに登録できるため、エンドポイントが最初のピアとの接続を失った場合、クラスタ内の別のピアに再登録できます。

容量の増加について

4つのピアの後に容量の増加はありません。そのため、たとえば6ピアのクラスタでは、5番目と6番目の Expressway がクラスタにコール キャパシティを追加することはありません。ピアを追加することで復元力は向上しますが、容量は向上しません。

小規模 Expressway VM は Cisco Business Edition 6000 の顧客を対象としているため、**小規模 VM のクラスタリングは冗長性のみを提供し、追加のスケールのメリットは提供しません。**

ライセンスについて

容量ライセンスはクラスタ単位で行われ、クラスタピアにインストールされたすべての容量ライセンスは、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およびルームシステムとデスクトップシステム登録ライセンスが含まれます。詳細については、「クラスタ内のライセンスの使用状況」を参照してください。



第 3 章

クラスタリングの要件

Expressway ピアのクラスタをセットアップするか、クラスタに Expressway を追加する前に、以下の要件が満たされていることを確認してください。

この章では、次の項目について説明します。

- [Expressway-C と Expressway-E を混在させないでください \(9 ページ\)](#)
- [プラットフォームとソフトウェアのバージョンが一致 \(9 ページ\)](#)
- [ネットワーク条件が満たされている \(10 ページ\)](#)
- [基本設定が完了しました \(10 ページ\)](#)
- [DNS 構成が完了しました \(11 ページ\)](#)
- [TMS 設定済み \(必須の場合\) \(12 ページ\)](#)
- [CE1200 および CE1100 物理アプライアンスが混在するクラスタ \(12 ページ\)](#)
- [Expressway と Expressway Select によるクラスタ導入の混在 \(12 ページ\)](#)

Expressway-C と Expressway-E を混在させないでください

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。同じクラスタに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のバージョンが一致

- すべてのクラスタ ピアは、同じ Expressway ソフトウェア バージョンを実行しています。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ケースは、クラスタがあるバージョンのコードから別のバージョンにアップグレードされている間の短期間であり、その間クラスタはパーティション分割された方法で動作します。
- 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、標準のアプライアンスで実行されているピアと 2 コアの中型の 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が、標準のアプライアンスで実行されているピアと、8 コアの大型 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

- 各ピアには異なる LAN 構成があります (有効になっている場合、異なる IPv4 アドレスおよび異なる IPv6 アドレス)。
- Expressway は最大 80ms の往復遅延をサポートします。これは、クラスタ内の各 Expressway は、クラスタ内の他のすべてのピアの 40ms ホップ以内でなければならないことを意味します。
- クラスタの各ピアは、クラスタ内の、またはクラスタに追加される他のすべての Expressway に直接ルーティング可能です。(クラスタ ピア間に NAT があってはなりません。ファイアウォールがある場合は、必要なポートが開いていることを確認してください。)
- 外部ファイアウォールが、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る。
- 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は信頼できる必要があります。

クラスタリング手順は正しい順序で実行される必要があります、プライマリピアが最初に起動する必要があります。他のピアが先に開始された場合、それらのピアがクラスタのコントロールを引き継ごうとする可能性があり、結果として復元が困難な不整合な設定状態になります。

基本設定が完了しました

- 各ピアには、他のすべてのピアとは異なるシステム名が付けられます。
- すべてのクラスタ ピアを同じドメインに設定します。
- 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の最低必要条件)。



(注) 1つのクラスタ内の複数の Expressway に対して1つの証明書を使用することをサポートしていますが、セキュリティ上のリスクがあるため、お勧めできません。つまり、1つのデバイスで1つの秘密鍵が危険にさらされた場合、クラスタ内のすべてのデバイスが危険にさらされます。

- オプションキーを引き続き使用するシステムがある場合、以下の例外を除き、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ています。
 - RMS ライセンス

- ルームシステム登録ライセンス
- デスクトップシステム登録ライセンス
- 各ピア ([設定 (Configuration)] > [プロトコル (Protocols)] > [H.323] で H.323 モードを有効にし、H.323 モードで [オン (On)] を選択します)。
クラスタは、すべてのエンドポイントが SIP エンドポイントの場合でも、ピア間で H.323 シグナリングを使用して、通話の最適なルートを決定します。
- 各ピアでファイアウォールルールを設定し、ピアを除くすべての IP アドレスからクラスタリング用の TLS ポートへの接続をブロックします。

DNS 構成が完了しました

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 ピアが使用する 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 ルックアップ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。
 - DNS 名を使用して設定されている場合、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
 - LDAP サーバーの正引きおよび逆引き (逆引きは PTR レコードにより頻繁に提供されます)



- (注) Expressway-E は通常、パブリック DNS を使用しますが、パブリック DNS を使用して **プライベート IP アドレス** を解決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リングすることも望ましくありません。これらの理由により、ピアの FQDN を **プライベート IP アドレス** に解決するために、クラスタアドレスマッピングを使用することを推奨します。

詳細は、「[Cisco Expressway シリーズ設定ガイド](#)」ページで、お使いのバージョンの『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。

- クラスタには、各ピアの A または AAAA レコードを含む DNS SRV レコードをお勧めします。

この設定は、ビデオ相互運用性および企業間 (B2B) のビデオ通話には推奨しますが、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対して、collab-edge SRV レコードを作成します。
- (B2B のみの場合) Expressway-E クラスタには、すべてのクラスタのピアを定義する DNS SRV レコードがあります。

TMS 設定済み (必須の場合)

- Cisco TMS を使用している場合、バージョン 13.2 以降が実行されていること (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 以降が許可されます)。
- FindMe データやプロビジョニングデータの複製に Cisco TMS を使用する場合は、Cisco TMS で Provisioning Extension モードの機能が有効になっていることを確認してください (詳細については、『[Cisco TMS Provisioning Extension 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 モデルを含む既存のクラスタに CE1200 アプライアンスを追加するには、[タイプ (Type)] オプションを、

[ステータス (Status)] > [概要 (Overview)] ページのサービスセットアップウィザードを通じて、CE1200 をクラスタに追加する前に、他のピアに一致するように設定します。

アプライアンスタイプが混在するクラスタがある場合、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、アプライアンスインストールガイドで、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かどうかを確認してください。

Expressway と Expressway Select によるクラスタ導入の混在



- (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は、Expressway ソフトウェア イメージまたは Expressway Select ソフトウェア イメージのいずれかを実行する必要があります。



第 4 章

クラスタを形成する方法

この章では、次の項目について説明します。

- [概要 \(13 ページ\)](#)

概要

- プライマリを含めて、クラスタ内に最大 6 つの Expressway を持つことができます。
- ピアを 1 つずつクラスタに追加します。
- 構成の変更はプライマリ Expressway でのみ行ってください。



注意 すべてのピアが実行されている状態でクラスタが安定するまで、クラスタ全体の設定を調整しないでください。クラスタの構成を変更したときに、ピアがアップグレード、再起動、またはサービス停止中の場合、クラスタデータベースのレプリケーションに悪影響が及びます。

他のピアに加えられた変更はクラスタ全体に反映されず、次回プライマリの設定がピア全体に複製される際に上書きされます。唯一の例外は、一部の [ピア固有の構成アイテム](#) です。

クラスタ内のすべてのピアに変更が更新されるまで、最大で 1 分待つ必要がある場合があります。

- クラスタ通信障害のアラームは、クラスタの形成中に発生します。終了するとアラームが解除されます。
- 新しい Expressways への構成のレプリケーションは、クラスタに適切に参加する前に中断されます。
- 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 \(Peer N address\)](#)] は外部インターフェースを指定してはいけません。ピア間に TLS を強制する必要がある場合 (つまり、TLS 検証が [[オン \(ON\)](#)] になっている)、ピアの

証明書に表示されるピアの FQDN をピア N アドレスに使用する必要があります。FQDN の DNS 解決はパブリック IP アドレスに解決される可能性が高いため、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。「[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、FQDN をプライベート IP アドレスにマッピングしてください。

- Expressway サーバーが単一の NIC を持ち、サーバーで静的 NAT が有効になっている場合、**[ピア N アドレス (Peer N address)]** は静的 NAT アドレスであってははいけません。ピア間に TLS を強制する必要がある場合（つまり、TLS 検証が **[オン (ON)]** になっている）、ピアの証明書に表示されるピアの FQDN をピア N アドレスに使用する必要があります。FQDN の DNS 解決はパブリック IP アドレスに解決される可能性が高いため、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。「[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、FQDN をプライベート IP アドレスにマッピングしてください。

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から外します。
 - メンテナンスモード (**[メンテナンス (Maintenance)] > [メンテナンスモード (Maintenance mode)]**) を有効にし、このピアですべての呼び出しが完了し、登録がタイムアウトになるまで待機します。
 - Expressway がクラスタ内にある場合、既存のクラスタから削除して再起動します。
 - Expressway を初期化します（前のステップで再起動したため、すでに行っている場合を除く）。
- 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てください。
- Expressway が他の Expressway のネイバー、トラバーサルクライアント、トラバーサルサーバーでないことを確認します。
- 設定をレビューおよび変更し、Expressway に以下があることを確認します。
 - 有効なイーサネット速度 (システム > ネットワークインターフェース > イーサネット)
 - 有効な IP アドレスおよび IP ゲートウェイ (システム > ネットワークインターフェース > IP)。
 - 有効で機能している NTP サーバーが設定されている (**[システム (System)] > [システム (Time)]**、**[ステータス (Status)]** セクションで **[状態 (State)]** が **[同期済み (Synchronized)]** である必要があります)。
 - 少なくとも 1 つの有効な DNS サーバーが設定されており、非修飾 DNS 名が他の場所 (NTP サーバーなど) で使用されている場合、正しいドメイン名も設定されている (非修飾 DNS 名にドメイン名をサフィックスとして追加して FQDN にします) (**[システム (System)] > [DNS]**)。

- [システム (System)]>[DNS]に移動し、[システムホスト名 (System host name)]がこの Expressway の DNS ホスト名であることを確認します ([システム名 (System name)] (通常は [システム (System)]>[管理 (Administration)]) と同じですが、スペースを除き、クラスタ内の各 Expressway に固有です)。正しく設定されていない場合は、適切に設定して [保存] をクリックします。



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

- ピアが設定されていません ([システム (System)]>[クラスタリング (Clustering)] - このページのすべての [ピア N アドレス (Peer N address)] フィールドが空欄になっています)。



注意

クラスタリング ページからすべてのピア アドレス フィールドを消去し、構成を保存した場合、Expressway は次に再起動を行ったときに、工場出荷時の状態にリセットされます。これは、LAN1 インターフェイスの基本的なネットワーク以外の既存のすべての設定を失うことを意味します。これには、フィールドをクリアしてから次の再起動までに行ったすべての設定が含まれます。

この Expressway がすでにクラスタのメンバーである場合、そのクラスタから削除し、別のクラスタで使用する前に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の場合は、クラスタの他のすべてのピアにインストールされるもの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てください(メンテナンス>オプションキー)。コール/RMS/デバイス/会議室ライセンスの数はピア間で異なる場合があります。他のすべてのライセンスキーは各ピアで同一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 ([設定 (Configuration)]>[プロトコル (Protocols)]>[H.323])
- この Expressway が Cisco TMSPE と統合されたクラスタに参加する場合、Expressway を Cisco TMS に追加し、以下を行います。
 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)]に移動し、[ステータス (Status)]セクションで、[状態 (State)]が「アクティブ」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 (System)]>[ナビゲータ (Navigator)] (および必要なサブフォルダ) に移動します。
 2. この Expressway を選択します。

3. [接続] タブを選択します。
4. この下位ピアの FQDN を **ホスト名** に設定します (例: vcs3.uk.company.com)。
5. [保存 (Save)]/[試行 (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>」のようなエラーメッセージは無視できます。

6. Cisco TMS が DNS を更新していることを確認します。
 1. [設定] タブを選択します。
 2. [強制更新] 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) に移動し、Expressway の名前をクリックして、以下が表示されていることを確認します。

「システムにはオープンチケットも承認済みチケットもありません」

- [システム > アラーム] に移動してください。Expressway を再起動する必要があるというアラームが表示された場合、[メンテナンス (Maintenance)] > [再起動 (Restart)] オプションに移動して、[再起動 (Restart)] をクリックします。

Expressway ピアの新しいクラスタを作成する

このプロセスは、単一の Expressway のクラスタを開始します。クラスタがすでに存在する場合は、このプロセスを使用しないでください。



重要 まず1つの(プライマリ)ピアのクラスタを作成し、他のピアを追加する前に、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」を確立したら、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 ピアは、クラスタ内のすべての Expressway ピアの構成情報のソースになります。下位の Expressway ピアでは、構成のほとんどが削除され、プライマリの構成によって置き換えられます。
2. Expressway が最新の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)] > [バックアップと復元 (Back and restore)])。
4. 構成を見直して変更し、Expressway に以下があることを確認します。
 - 有効なイーサネット速度 (システム > ネットワークインタフェース > イーサネット)

- 有効な IP アドレスおよび IP ゲートウェイ (システム > ネットワークインターフェース > IP)。
- 有効で動作している NTP サーバーが構成されています (システム > 時刻; ステータス セクションで、State は「Synchronized」である必要があります)。
- 少なくとも 1 つの有効な DNS サーバーが設定されており、非修飾 DNS 名が他の場所 (NTP サーバーなど) で使用されている場合、正しいドメイン名も設定されている (非修飾 DNS 名にドメイン名をサフィックスとして追加して FQDN にします) ([システム (System)] > [DNS])。
- [システム (System)] > [DNS] に移動し、[システムホスト名 (System host name)] がこの Expressway の DNS ホスト名であることを確認します ([システム名 (System name)] (通常は [システム (System)] > [管理 (Administration)]) と同じですが、スペースを除き、クラスタ内の各 Expressway に固有です)。正しく設定されていない場合は、適切に設定して [保存] をクリックします。



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

- ピアが設定されていません ([システム (System)] > [クラスタリング (Clustering)] - このページのすべての [ピア N アドレス (Peer N address)] フィールドが空欄になっています)。



注意

クラスタリング ページからすべてのピア アドレス フィールドを消去し、構成を保存した場合、Expressway は次に再起動を行ったときに、工場出荷時の状態にリセットされます。これは、LAN1 インターフェイスの基本的なネットワーク以外の既存のすべての設定を失うことを意味します。これには、フィールドをクリアしてから次の再起動までに行ったすべての設定が含まれます。

この Expressway がすでにクラスタのメンバーである場合、そのクラスタから削除し、別のクラスタで使用する前に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の場合は、クラスタの他のすべてのピアにインストールされるもの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てください (メンテナンス > オプションキー)。コール/RMS/デバイス/会議室ライセンスの数はピア間で異なる場合があります。他のすべてのライセンスキーは各ピアで同一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 ([設定 (Configuration)] > [プロトコル (Protocols)] > [H.323])

5. この Expressway が、新しいクラスタのピアとなる Expressway をその近隣ゾーンまたはトラバーサルゾーンにリストしないことを確認し ([設定 (Configuration)] > [ゾーン (Zones)] > [ゾーン (Zones)])、各近隣とトラバーサルゾーンを確認します。

6. [**H.323 有効時間**] を展開のサイズに適した値に設定します。60 秒など、より小さい数値を設定すると、1 つの Expressway がアクセス不能になった場合に、エンドポイントがすぐに別のピアに登録されます ([**設定 (Configuration)**] > [**プロトコル (Protocols)**] > [**H.323**])。



(注) 登録の有効期限を短くしすぎると、Expressway に登録要求が殺到し、パフォーマンスに深刻な影響を与える危険性があります。この影響はエンドポイントの数に比例するため、時折の迅速なフェイルオーバーと、継続的な良好なパフォーマンスの必要性のバランスをとってください。

7. [**システム (System)**] > [**DNS**] に移動し、[**システムホスト名 (System host name)**] がこの Expressway の DNS ホスト名であることを確認します ([**システム名 (System name)**] (通常は [**システム (System)**] > [**管理 (Administration)**]) と同じですが、スペースを除き、クラスタ内の各 Expressway に固有です)。正しく構成されていない場合は、適切に設定して [**保存**] をクリックします。



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

8. [**設定 (Configuration)**] > [**通話ルーティング (Call routing)**] に移動し、[**コールシグナリングの最適化 (Call signaling optimization)**] を [**オン (On)**] に設定します。
9. [**保存 (Save)**] をクリックします。
10. **メンテナンスモード** ([**メンテナンス (Maintenance)**] > [**メンテナンスモード (Maintenance mode)**]) を有効にし、このピアですべての呼び出しが完了し、登録がタイムアウトになるまで待機します。
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)**] に移動し、[**クラスタ名 (Cluster name)**] がこの Expressway クラスタをアドレス指定する 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であることを確認します (cluster1.example.com など) (「[クラスタ名および DNS SRV レコード](#)」を参照)。
必要に応じて **クラスタ名** を変更します。
12. [**保存 (Save)**] をクリックします。
13. [**クラスタリング**] ページでフィールドを次のように設定します:

設定プライマリ	1
クラスタ IP バージョン	ネットワークアドレス指定スキームに合わせて IPv4 または IPv6 を選択してください。

<p>TLS 検証モード</p>	<p>オプション: [許可 (Permissive)] (デフォルト) または [強制 (Enforce)]。</p> <p>[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。</p> <p>[強制] はより安全ですが、各ピアが有効な証明書を持ち、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。</p> <p>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。[許容 (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] に切り替えることができます。</p> <p>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、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 クラスタのためのクラスタアドレスマッピング」を参照してください。</p>
<p>ピア 1 アドレス</p>	<p>この Expressway (プライマリピア) のアドレスを入力します。</p> <p>[TLS 検証モード (TLS verification mode)] が [強制 (Enforce)] に設定されている場合、サブジェクト CN に一致する FQDN またはこのピアの証明書上の SAN を入力する必要があります。</p>

14. [保存 (Save)] をクリックします。
[ピア 1 アドレス (Peer 1 address)] フィールドの右側に、「このシステム (This system)」と表示されます (表示される前にページを更新する必要があります)。
15. Expressway を再起動します ([メンテナンス (Maintenance)] > [再起動オプション (Restart options)] に移動し、[再起動 (Restart)] をクリックして [OK] を確認します)。
16. 構成データが適切に存在することを確認します。
 - FindMe が使用されている場合、予期される FindMe エントリがまだ存在していることを確認します ([ステータス (Status)] > [アプリケーション (Applications)] > [TMS Provisioning Extension サービス (TMS Provisioning Extension Services)] > [FindMe] > [アカウント (Accounts)])。
 - [システム (System)]、[設定 (Configuration)]、および [アプリケーション (Application)] メニューからの項目の設定を確認します。
17. メンテナンスモードが無効になっていることを確認してください。
 1. メンテナンス > メンテナンスモードに移動してください。

2. メンテナンスモードをオフに設定します。
3. [保存 (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 > バックアップと復元)。

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 > アラーム] に移動し、すべてのアラームが対処され、解除されていることを確認します。
- [[クラスタにピアを追加 (Add a Peer to a Cluster)]] 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する

この手順は既存のクラスタ (1 つまたは複数のピア) 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を作成する](#)」を参照してください。

1. プライマリ Expressway で [システム > クラスタリング] に移動します。
1 つ以上の [ピア N アドレス (Peer N address)] フィールドが空である必要があります。
2. 最初の空のフィールドで、新しい Expressway ピアの入力します。
3. [保存 (Save)] をクリックします。
ピア 1 は「このシステム」を示す必要があります。新しいピアは「不明」を示す可能性があり、その後、クラスタに完全に参加していないため、更新で「失敗」と示されます。
4. すでにクラスタ内にある下位のピアの 1 つで [システム > クラスタリング] に移動し、次のフィールドを編集します:

クラスタ名	プライマリ Expressway で設定された クラスタ名 と同一のもの
設定プライマリ	プライマリ Expressway で選択されたのと同じ番号
クラスタ IP バージョン	プライマリ Expressway で選択されたのと同じバージョン
TLS 検証モード	プライマリ Expressway* で選択されたのと同じ設定

ピア 1 アドレス ... ピア 6 アドレス	アドレスは、プライマリ Expressway で入力されたものと同じであり、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予定がある場合、クラスタ内のすべてのデバイスは、最初に許可モードになっている必要があります。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。

- すでにクラスタ内にある各下位ピアに対して、前の手順を繰り返します。
- 新しいピアで [システム > クラスタリング] に移動します:

クラスタ名	プライマリ Expressway で設定された クラスタ名 と同一のもの
設定プライマリ	プライマリ Expressway で選択されたのと同じ番号
クラスタ IP バージョン	プライマリ Expressway で選択されたのと同じバージョン
TLS 検証モード	プライマリ Expressway* で選択されたのと同じ設定
ピア 1 アドレス ... ピア 6 アドレス	アドレスは、プライマリ Expressway で入力されたものと同じであり、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予定がある場合、クラスタ内のすべてのデバイスは、最初に許可モードになっている必要があります。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。

- Expressway がクラスタ通信障害のアラームを生成します。必要な再起動後にアラームはクリアされます。
- Expressway を再起動します ([メンテナンス (Maintenance)] > [再起動オプション (Restart options)]) に移動し、[再起動 (Restart)] をクリックして [OK] を確認します)。

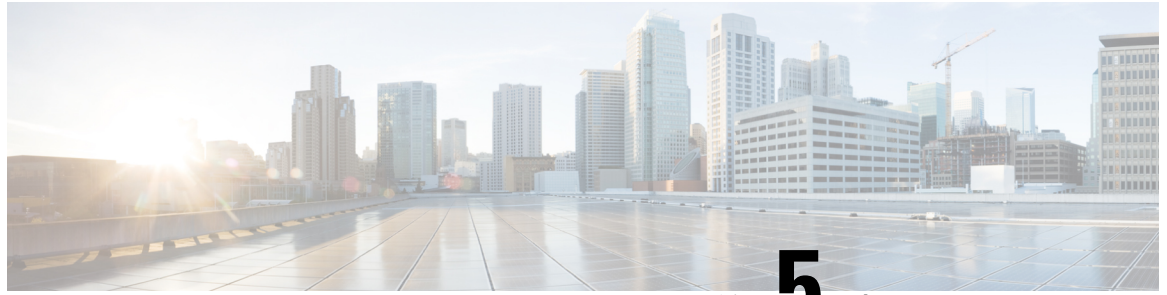
確認

- 再起動後、約 2 分待機します。これは、プライマリから設定がコピーされる頻度です。
- クラスタデータベースの状況を確認してください。
- 構成データが適切に存在することを確認します。

- FindMe が使用されている場合、予期される FindMe エントリがまだ存在していることを確認します ([ステータス (Status)] > [アプリケーション (Applications)] > [TMS Provisioning Extension サービス (TMS Provisioning Extension Services)] > [FindMe] > [アカウント (Accounts)])。
- [システム (System)]、[設定 (Configuration)]、および [アプリケーション (Application)] メニューからの項目の設定を確認します。

次のステップ

- 必要に応じてピアを追加します。
- クラスタで会議ファクトリ (Multiway™) を使用している場合は、[クラスタリングが他の Expressway アプリケーションに与える影響](#)を参照してください。
- ピアに FQDN をプライベート IP アドレスに解決させたい場合は、「[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。



第 5 章

(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

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、ピア間の TLS 検証を強制する場合に必要です。クラスタを形成していない場合は、「[クラスタを形成する方法](#)」を参照してください。

Expressway-E のクラスタを作成している場合、DMZ などの隔離されたネットワークにある可能性があります。TLS 検証を実施する場合は、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、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、次の項目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 \(23 ページ\)](#)
- [クラスタアドレスマッピングの構成 \(Expressway-E クラスタ\) \(25 ページ\)](#)
- [FQDN を使用するようにクラスタを変更する \(26 ページ\)](#)
- [TLS 検証の強制 \(29 ページ\)](#)

Expressway-E クラスタのクラスタアドレスマッピング

MRA のようなセキュアな展開の場合、各 Expressway-E ピアにはパブリック FQDN を含む SAN の証明書が必要です。FQDN はパブリック 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 エンドポイントのような外部エンティティは、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か

- 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必要ありません。

- クラスタ内の Expressway-E ピアに、証明書を使用して互いのアイデンティティを確認させたい場合、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。Expressway-E ノードが NIC を 1 つだけ持ち、静的 NAT を使用しておらず、ルーティング可能な IP アドレスを持っている場合、これはクラスタを形成するための完全に許容可能な方法です。クラスタ アドレス マッピングは必要ありません。
- セキュリティポリシーがピア間の TLS 検証を強制することを指示している場合、および Expressway-E が静的 NAT、またはデュアル NIC、またはその両方を使用している場合、クラスタから外部インターフェイスまたは静的 NAT アドレスを使用することは推奨しません。

また、パブリック 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。外部接続が切断されるためです。

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、ピアはこれらの名前を IP アドレスに変換する必要があります。この変換が DNS の主な理由ですが、ピアが 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を設定して、DNS のローカルな代替値を提供できます。

クラスタ アドレス マッピングは FQDN:IP ペアで、クラスタ全体で共有されます (各ピアに対して 1 ペア)。ピアは DNS にクエリを実行する前に、マッピング テーブルを参照し、一致が見つかった場合、DNS にクエリを実行しません。

TLS を強制することを選択した場合、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。

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行う唯一の方法です。

推奨されるマッピングの出所

クラスタがすでに IP アドレスを使用して形成されており、ピアがすでにシステムのホスト名と DNS 名を [システム (System)] > [DNS] ページで設定している場合、次のように想定されるマッピングをクラスタアドレスマッピングテーブルに自動的に入力するオプションがあります。

Peer1Hostname.Peer1DNSName のマッピング先 <Peer1 Private IP address>

...

Peer6Hostname.Peer6DNSName のマッピング先 <Peer6 Private IP address>



- (注) この自動マッピングは間違っている可能性があります。ピアの証明書の SAN フィールドにこれらの想定される FQDN が含まれていない場合、**[TLS 検証モード (TLS verification mode)]** が **[強制 (Enforce)]** に変更されると、クラスタが形成されません。ピア FQDN フィールドに配置したエントリが 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通して動的に複製します。

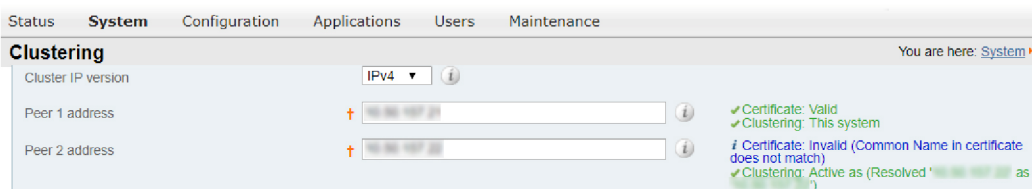
マッピングの順序は重要ではありませんが、アドレスマッピングを使用している場合は、すべてのクラスタピアに対してマッピングを作成し、**プライベート IP アドレスのみ**を使用する必要があります。

手順

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

ステップ 2 ピアアドレス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確認して、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 **[証明書: 無効 (Certificate: Invalid)]** ...ステータス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ために証明書が正しく形成されていると想定して、証明書が内部/プライベート IP アドレスと対応するべきではないためです。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 プライマリピアの **[システム (System)]** > **[クラスタリング (Clustering)]** に移動し、**[クラスタアドレスマッピングが有効 (Cluster address mapping enabled)]** ドロップダウンを **[オン (On)]** (デフォルトは **[オフ (Off)]**) に変更します。

クラスタアドレスマッピング フィールドが表示されます。

FQDN を使用するようにクラスタを変更する

ステップ 4 [オプション、上記のメモを参照] [システム情報に基づいてマッピングを提示 (Suggest mappings based on system information)] をクリックし、各クラスタピアのマッピングフィールドを自動入力します。これは、各ピアの [システム (System)] > [DNS ページ (DNS pages)] で設定された [システムホスト名 (System host name)] と [DNS 名 (DNS name)] を使用し、それらを内側向きの 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、およびクラスタリングする 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 DNS と一致しない情報に基づいて構築されます。)

ステップ 6 Expressway-E ピアのパブリック FQDN が内部に面する 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、または DNS を照会することで、パブリック FQDN を確認できます)。

ステップ 7 [保存 (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)

クラスタはまだ IP アドレスを使用して形成されており、TLS 検証の [許可 (Permissive)] モードをまだ使用しています。[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する

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 ([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) に入力されているアドレスを使用します。



(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、クラスタが新しいアドレスに一致するまで、アラームが表示され続けます。

手順

ステップ 1 すべてのクラスタピアにサインインし、それぞれで [システム (System)] > [クラスタリング (Clustering)] に移動します。

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すすめします。

ステップ 3 クラスタ内の各ピア:

- 選択したピアアドレスフィールドを IP アドレスから対応する FQDN に変更します (マッピングを行っている場合、この段階ですべてのピアでマッピングを複製する必要があります)。
- **[保存 (Save)]** をクリックします。

注意

各ボックスで1つのピアアドレスのみを変更するようにしてください。

ステップ 4 現在変更しているピアアドレスで識別されるピアに切り替え、このピアを再起動 (**[メンテナンス (Maintenance)] > [再起動オプション (Restart options)]** に移動) した後、**[再起動 (Restart)]** をクリックし、**[OK]** をクリックして確認します。

(注)

すべてのピアでピアアドレスを変更する場合、1回の再起動が必要です。

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ちます。

クラスタ全体で、このピアのクラスタリングアドレスを IP アドレスから FQDN に正常に変更しました。

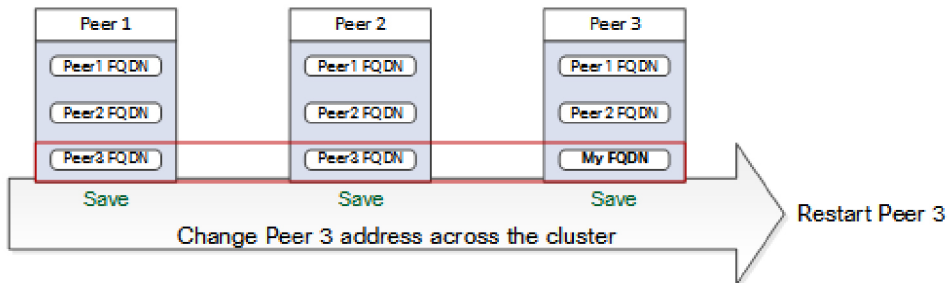
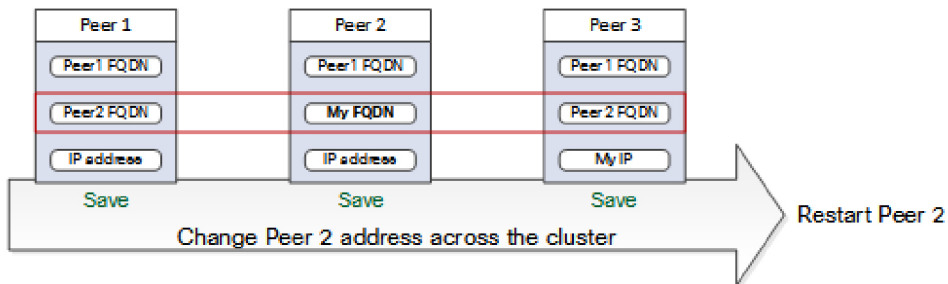
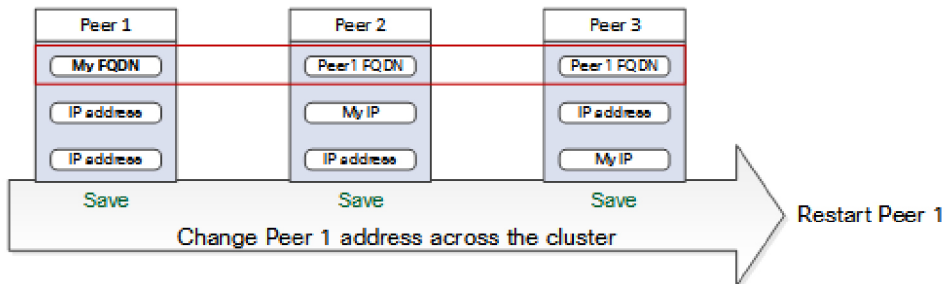
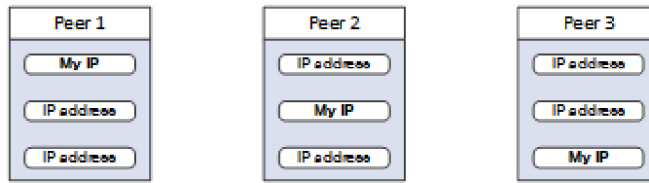
ステップ 6 次に変更するピアアドレスを選択し、ステップ 3 ~ 5 を繰り返します。すべてのピアアドレスを変更し、すべてのピアを再起動するまで、このループを繰り返します。

クラスタ全体が FQDN で動作しているはずですが、クラスタはまだ許可モードのままです。

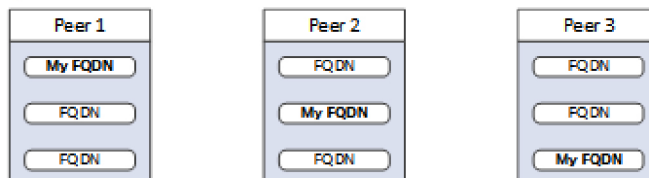
クラスタが Expressway-E クラスタで、ピア間で TLS 検証を強制することを目指している場合、ピアアドレスフィールドは証明書で提示されたアイデンティティと一致する必要があります。クラスタリングと証明書の両方のステータスメッセージが緑であることを確認します。

FQDN を使用するようにクラスタを変更する

Start: "IP Permissive" cluster



End: "FQDN Permissive" cluster



445424

TLS 検証の強制

事前準備



注意 証明書 SAN に、ピア N アドレス フィールドにある 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 フィールドの隣に、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るはずですが。

TLS 検証を強制するプロセス

手順

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

証明書が無効な場合、警告が表示され、クラスタが強制 TLS 検証モードで適切に動作することを妨げます。

新しい TLS 検証モードはクラスタ全体で複製されます。

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

ステップ 3 [保存] をクリックして、プライマリピアを再起動します。

ステップ 4 他の各ピアにサインインし、ピアを再起動します。

ステップ 5 クラスタが安定するのを待ち、すべてのピアについて、クラスタリングと証明書のステータスが緑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

これは初期セットアップではなく、運用上の使用方法に関するものですが、便宜上、ここで説明します。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、受け取った証明書を検証するために、CN (共通名) ではなく、SAN 属性 (サブジェクト代替名) を使用します。



第 6 章

クラスタを変更する方法

クラスタが他のシステムに接続されている場合、クラスタへの変更が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ときは、次のことに注意してください。

- このクラスタの近隣、クライアント、またはサーバーである他の Expressway を確認し、ゾーン設定を更新します。たとえば、このクラスタにピアを追加または削除する場合、このクラスタに対する近隣ゾーンのピア アドレス リスト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 はクラスタへのトランクを持っている場合があります。または、新しいクラスタピアで更新され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 クラスタに登録するエンドポイントが新規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均等に登録できるようにします。
- ピアを追加または削除した場合、あるいは IP アドレスまたは FQDN を変更した場合、このクラスタの 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 モデルを含む既存のクラスタに CE1200 アプライアンスを追加するには、サービスセットアップウィザードを通じて、他のピア (Expressway-E または Expressway-C) と一致するように [タイプ (Type)] オプションを [ステータス (Status)] > [概要 (Overview)] ページで、CE1200 をクラスタに追加する前に設定します。

クラスタの既存のアプライアンスより新しいモデルを追加する場合、新しいアプライアンスに後で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、それが作成されたのと同じソフトウェアバージョン上にものみ復元できます。) **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の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のバージョンをサポートできるかどうかを確認してください。

- SAML メタデータを再エクスポートして IDP にコピーしてください。Expressway-C のクラスタでピアを追加、削除、または置換するたびに、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 は一時的に失敗します。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を生成するために使用されるためです。詳細については、「[Expressway 設定ガイド](#)」ページの「[Cisco Expressway を介したモバイルおよびリモートアクセスに関する導入ガイド](#)」を参照してください。



(注) 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十分ではないため、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。



(注) 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、次の項目について説明します。

- [クラスタを変更する前に](#) (32 ページ)
- [クラスタからライブピアを \(永久に\) 削除する](#) (33 ページ)
- [クラスタからデッドピアを \(永久に\) 削除する](#) (35 ページ)
- [Expressway クラスタピアの復旧](#) (37 ページ)
- [クラスタの解除](#) (37 ページ)
- [プライマリピアの変更](#) (38 ページ)
- [ピアアイデンティティの変更](#) (39 ページ)
- [ピアの置き換え](#) (40 ページ)

クラスタを変更する前に

- ピアとして設定されているシステムは、お互いにネイバーとして設定してはいけません。その逆も同様です。
- ピアが異なる LAN に展開されている場合、ピア間の遅延を低く抑えるために、ネットワーク間に十分な接続性がなければなりません。
- クラスタピアは別々のサブネットに存在できます。ピアは、サブネットの境界を越えて送信できる H.323 メッセージングを使用して相互に通信します。
- 同じ LAN 上のクラスタ内のすべてのピアを展開するということは、ローカルドメイン名およびローカルドメインサブネットマスクなどの同じルーティング情報で構成できることを意味します。

- 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 フィールドを消去し、保存してから再起動します。



注意 クラスタリング ページからすべてのピア アドレス フィールドを消去し、構成を保存すると、次に再起動を行うときに、Expressway は工場出荷時設定にリセットされます。これは、LAN1 インターフェイスの基本的なネットワークを除く既存のすべての構成を失うことを意味します。これには、フィールドの消去と次の再起動の間に行ったすべての構成が含まれます。

Expressway は、工場出荷時設定へのリセットが保留中であることを知らせるバナーを表示しません。

工場出荷時設定へのリセットを防ぐ必要がある場合は、クラスタリング ピア アドレス フィールドを元の状態に復元します。元のピア アドレスを同じ順序で置き換え、設定を保存してバナーを消去し、リセットを防ぎます。

クラスタからライブピアを（永久に）削除する

このプロセスは、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。
- 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（永久に）削除する \(35 ページ\)](#) を参照してください。
- Expressway クラスタピアを復元する場合は、[Expressway クラスタ ピアの復旧 \(37 ページ\)](#) を参照してください。

クラスタから削除する Expressway 上

手順

ステップ 1 [システム > クラスタリング] に移動します。

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]

注意

クラスタリング ページからすべてのピア アドレス フィールドを消去し、構成を保存すると、次に再起動を行うときに、Expressway は工場出荷時設定にリセットされます。これは、LAN1 インターフェイスの基

本的なネットワーク以外の既存のすべての設定を失うことを意味します。これには、フィールドをクリアしてから次の再起動までに行ったすべての設定が含まれます。

工場出荷時設定へのリセットを回避する必要がある場合は、クラスタリング ピア アドレス フィールドを元に戻してください。元のピアアドレスを同じ順序で置換し、設定を保存してバナーを消去します。

ステップ 4 Expressway を再起動します ([メンテナンス (Maintenance)] > [再起動オプション (Restart options)] に移動し、[再起動 (Restart)] をクリックして [OK] を確認します)。

工場出荷時設定へのリセットは、ピアの再起動時に自動的にトリガーされ、機密データとクラスタ構成を削除します。リセットにより、以下にリストされている基本ネットワーク情報を除くすべての構成が消去されます。これらの情報は LAN1 インターフェイスに保存されるため、Expressway にアクセスできます。デュアル NIC オプションを使用する場合、LAN2 設定はリセットにより完全に削除されることに注意してください。

リセット後に保存される設定 (LAN1):

- IP アドレス
- Admin および root アカウントとパスワード
- SSH キー
- オプション キー
- HTTPS アクセスが有効です
- [SSH アクセス有効 (SSH access enabled)]

(注)

バージョン X12-6 から、工場出荷時設定へのリセットは、サーバー証明書、関連する秘密鍵、および CA トラストストア設定をピアから削除します。以前の Expressway ソフトウェアバージョンでは、これらの設定は保存されていました。

プライマリ Expressway 上

手順

ステップ 1 [システム > クラスタリング] に移動してください。

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 削除される Expressway がリストの最後のフィールドではない場合、他のアドレスをリスト内で上に移動して、エントリの間空のフィールドがないようにします。

ステップ 4 前のステップでプライマリ Expressway ピアのアドレスがリストの上に移動された場合、[設定プライマリ (Configuration primary)] 値を新しいロケーションに合わせて変更します。

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

手順

ステップ1 [システム > クラスタリング] に移動します。

ステップ2 ピア N アドレス および 構成のプライマリ フィールドを編集して、プライマリ Expressway で設定されたものと同一になるようにします。

ステップ3 [保存 (Save)] をクリックします。

ステップ4 残りのすべての下位 Expressway ピアに対して、同一のクラスタリング構成になるまで繰り返します。
クラスタからのライブ Expressway の削除が完了しました。

クラスタからデッドピアを（永久に）削除する

この手順により、RMA が必要な場合、またはその他の理由でアクセスできない場合、サービス停止中のピアをクラスタから削除します。

- 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、[クラスタからライブピアを（永久に）削除する \(33 ページ\)](#) 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 ピアを復元する場合は、[Expressway クラスタ ピアの復旧 \(37 ページ\)](#) を参照してください。



(注) この手順では Expressway からの構成は消去されません。システムの復元に成功した場合でも、デフォルト設定にリセットする (ファクトリーリセット) までは、そのシステムを使用してはいけません。

プライマリ Expressway:

1. [システム > クラスタリング] に移動してください。
2. 削除された Expressway のアドレスを削除します。

3. 削除される Expressway がリストの最後のフィールドではない場合、他のアドレスをリスト内で上に移動して、エントリの上に空のフィールドがないようにします。
4. 前のステップでプライマリ Expressway ピアのアドレスがリストの上に移動された場合、**[設定プライマリ (Configuration primary)]** 値を新しいロケーションに合わせて変更します。
5. **[保存 (Save)]** をクリックします。

残りのすべての下位の Expressway ピアで:

1. システム > クラスタリングに移動します。
2. **[ピア N アドレス (Peer N address)]** フィールドと **[設定プライマリ (Configuration primary)]** フィールドを編集し、プライマリ Expressway で設定されたものと同一になるようにします。
3. **[保存 (Save)]** をクリックします。
4. 残りのすべての下位 Expressway ピアに対して、同一のクラスタリング構成になるまで繰り返します。

Expressway クラスタからアクセス不能なピアを削除しました。

このピアの設定を消去

削除したピアを復元する場合、ネットワークに再接続する前にその設定を消去する必要があります。

手順

ステップ 1 **[システム (System)]** > **[クラスタリング (Clustering)]** に移動します。

ステップ 2 **[ピア N アドレス]** フィールドの入力内容をすべて削除してください。

ステップ 3 **[保存 (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)]** > **[再起動オプション (Restart options)]** に移動し、**[再起動 (Restart)]** をクリックして **[OK]** を確認します)。再起動を行うと、Expressway は工場出荷時設定へのリセットを開始します。以下を除き、削除されたすべての設定が復旧します。

工場出荷時設定へのリセットは、ピアの再起動時に自動的にトリガーされ、機密データとクラスタ構成を削除します。リセットにより、以下にリストされている基本ネットワーク情報を除くすべての構成が消去されます。これらの情報は LAN1 インターフェイスに保存されるため、Expressway にアクセスできます。デュアル NIC オプションを使用する場合、リセットにより LAN2 構成が完全に削除されることに注意してください。

リセット後に保存される設定 (LAN1):

- IP アドレス

- Admin および root アカウントとパスワード
- SSH キー
- オプション キー
- HTTPS アクセスが有効です
- [SSH アクセス有効 (SSH access enabled)]

(注)

バージョン X12-6 から、工場出荷時設定へのリセットは、サーバー証明書、関連する秘密鍵、および CA トラストストア設定をピアから削除します。以前の Expressway ソフトウェアバージョンでは、これらの設定は保存されていました。

これでクラスタに戻すことができます。次を参照してください。 [クラスタにピアを追加する \(20 ページ\)](#)

Expressway クラスタ ピアの復旧

Expressway はクラスタ内にあります。不本意にクラスタから外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、

- 再挿入する前に、ピアをクラスタから削除します
- クラスタリストの最後のピアにします
- そのようなピアのバックアップは、再挿入後の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 および設定レプリケーションが停止され、プロビジョニングも停止され、クラスタが Cisco TMS から削除されます。

各 Expressway はウェブ 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消去されます。

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設定を消去します。X8.11以降では、クラスタリング構成を消去することで、Expressway を工場出荷時設定にリセットするための準備を行います。「1つのクラスタ」として Expressway を設定する必要がある状況があるため、プライマリを初期化することを確信している必要があります。

クラスタを解除するには:

手順

-
- 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（永久に）削除する（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、Cisco TMS にログインし、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)] (および必要なサブフォルダ) を選択し、クラスタ内の任意の Expressway をクリックします。
 2. [プロビジョニング] タブを選択します。
 3. 4つのサービスをすべて無効にします (チェックボックスをオフにします)。
 4. [保存 (Save)] をクリックします。
- ステップ3** 配下のピアをそれぞれ順番に削除します。 [クラスタからライブピアを（永久に）削除する（33 ページ）](#) を参照してください。
- 最下位のピアを削除するとき、プライマリピアだけをクラスタに残す必要があります。
- クラスタは現在「1つのクラスタ」であり、この Expressway をその構成で保持する場合は、ここで停止できます。
- ステップ4** プライマリピアを出荷時設定にリセットする場合は、それにログインして、次のプロセスに従います [クラスタからライブピアを（永久に）削除する（33 ページ）](#)。
- クラスタの解除が完了しました。
-

プライマリピアの変更

現在のプライマリピアが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をめぐっ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に従うようにしてください。

通常、[設定プライマリ (Configuration primary)] を変更するだけで、プライマリ Expressway ユニットのサービスから外すか、元のプライマリピアが故障した場合に限ります。



(注) Cisco TMS には変更は必要ありません。Cisco TMS は Expressway クラスタのプライマリ変更を確認し、これを適切にレポートします。

手順

-
- ステップ 1** 「新しい」プライマリ Expressway で、[システム (System)] > [クラスタリング (Clustering)] に移動します。
- ステップ 2** 構成のプライマリ ドロップダウンメニューから、「このシステム」と表示されているピア エントリの ID 番号を選択します。
- ステップ 3** [保存 (Save)] をクリックします。
- プライマリピアを変更している間、「クラスタプライマリの不一致」または「クラスタレプリケーションエラー」を報告する Expressway のアラームを無視します。これらはこの手順の一部として修正されません。
- ステップ 4** 他のすべての Expressway ピアで、「古い」プライマリピア (アクセス可能な場合) から、[システム (System)] > [クラスタリング (Clustering)] に移動します。
- ステップ 5** [プライマリ設定] ドロップダウンメニューから、「新しい」プライマリ Expressway の ID 番号を選択します。
- ステップ 6** [保存 (Save)] をクリックします。
- 「クラスタのプライマリの不一致」および「クラスタのレプリケーションエラー」に関連する Expressway ピアで生成されたアラームは、約 2 分後に自動的にクリアされます。
- ステップ 7** [設定プライマリ (Configuration primary)] への変更が承認されたことを確認するには、[システム (System)] > [クラスタリング (Clustering)] に移動してページを更新します。
- ステップ 8** 変更を承認していない Expressway がある場合、上記の手順を繰り返します。
- ステップ 9** クラスタ データベースの状況が [アクティブ] としてレポートされることを確認します。
- ステップ 10** 「古い」プライマリ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 \(永久に\) 削除する \(35 ページ\)](#) 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可能性がある場合は、他のピアから隔離し、可能であれば工場出荷時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構成され、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。
-

ピアアイデンティティの変更

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 をクラスタに追加し直す必要があります。

プロセスは次のとおりです。

手順

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

それがプライマリ Expressway の場合、[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 [クラスタからライブピアを \(永久に\) 削除する \(33 ページ\)](#) に記載されたプロセスを実行します。

ステップ 3 Expressway の IP アドレス、ホスト名、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する \(20 ページ\)](#) に記載された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、この IP アドレス、ホスト名、または FQDN はクラスタリングに使用されないため、クラスタを解除する必要はありません。

ピアの置き換え

このセクションでは、異なるユニットでクラスタ ピア Expressway を置き換えるための手順を要約します。

手順

ステップ 1 置き換えられる Expressway がプライマリ Expressway でないことを確認します。

それがプライマリ Expressway の場合、[プライマリ ピアの変更 \(38 ページ\)](#) の手順に従い、別のピアをプライマリにします。

ステップ 2 クラスタから既存のピアを削除します。

1. 置換されるクラスタ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 \(永久に\) 削除する \(35 ページ\)](#) に定義されている手順を使用します。
2. 置換されるクラスタピアにアクセスできる場合は、[クラスタからライブピアを \(永久に\) 削除する \(33 ページ\)](#) に定義されている手順を使用します。

ステップ 3 [クラスタにピアを追加する \(20 ページ\)](#) に定義されている手順を使用して、置換ピアをクラスタに追加します。

重要

追加情報 (物理アプライアンスを持つクラスタがある場合)

CE1100 モデルを含む既存のクラスタに CE1200 アプライアンスを追加するには、サービスセットアップウィザードを通じて、他のピア (Expressway-E または Expressway-C) と一致するように [タイプ (Type)] オプションを [ステータス (Status)] > [概要 (Overview)] ページで、CE1200 をクラスタに追加する前に設定します。

クラスタの既存のアプライアンスより新しいモデルを追加する場合、新しいアプライアンスに後で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、それが作成されたのと同じソフトウェアバージョン上のみ復元できます。)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、アプライアンスのインストールガイドで、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に対応していることを確認してください。

ピアを置き換え、その構成を移行する

この手順は、アクセス可能な Expressway ピアを別の Expressway と置き換えることを想定しています。

手順

- ステップ 1** 置き換えられる Expressway がプライマリ Expressway でないことを確認します。
それがプライマリ Expressway の場合、[プライマリピアの変更 \(38 ページ\)](#) の手順に従い、別のピアをプライマリにします。
- ステップ 2** クラスタ設定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。[クラスタからライブピアを \(永久に\) 削除する \(33 ページ\)](#) を参照してください。
- ステップ 3** 再起動する前に、削除され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** 削除されたピアから新しい Expressway にバックアップを復元します。
- ステップ 6** 新しい Expressway の DNS 構成が他のピアと同じであることを確認し、それを同じ 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する \(20 ページ\)](#) で定義された手順を使用して、代替のピアをクラスタに追加します。
その手順に従うとき、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。
最も重要なステップの概要をここに示します。
 1. 古いピアのアドレスの代わりに新しいピアのアドレスをプライマリのクラスタリング設定に追加します。
 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設定を入力します(クラスタ名、共有シークレット、順序付きピアリスト)。

ステップ 8 新しいピアを再起動します。

ステップ 9 約 5 分待ってから、クラスタの状況を確認し、アラームがあれば解決します。

ステップ 10 削除されたピアを再起動して工場出荷時設定へのリセットを開始し、古い構成を消去します。



第 7 章

Expressway クラスタを他のシステムに接続する方法

この章では、次の項目について説明します。

- [Expressway クラスタ間の近隣](#) (43 ページ)
- [クラスタと連携するためのエンドポイントの設定](#) (43 ページ)
- [Expressway を Cisco TMS に追加する](#) (48 ページ)

Expressway クラスタ間の近隣

ローカルの Expressway クラスタをリモートの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の近隣、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の可能性があります。呼び出しがローカル Expressway で受信され、関連するゾーンを経由してリモートクラスタに渡されるとき、その近隣クラスタ内の最も低いリソース使用率を持つピアにルーティングされます（メンテナンスモードのピアは考慮されません）。そのピアは、通話を次のいずれかのピアに転送します。

- ローカルに登録されたエンドポイント (エンドポイントがピアに登録されている場合)
- ピア (エンドポイントがクラスタ内の別のピアに登録されている場合)
- 外部ゾーン (エンドポイントが別の場所にある場合)

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

クラスタと連携するためのエンドポイントの設定

エンドポイントを構成するとき、クラスタ内のすべての Expressway ピアについて知ることが望ましいです。そのため、初期登録時またはそれ以降、エンドポイントが Expressway ピアへの接続を失った場合に、クラスタ内の別のピアに登録できるようになります。このセクションでは、それぞれ SIP エンドポイントと H.323 エンドポイントで利用可能な構成方法を推奨する順番で一覧表示しています。

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 ダイアルのセクションを参照してください [クラスタ名および DNS SRV レコード \(61 ページ\)](#)。



(注) SIP および 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

オプションは、1 つまたは複数の Expressway クラスタピアがアクセス不能になった場合に、Expressway のクラスタへのエンドポイントの接続の耐障害性を提供するために優先順にリストされています。オプションの選択は、使用しているエンドポイントがサポートする機能によって異なります。

オプション 1 - SIP アウトバウンド (優先)



重要 Cisco Collaboration Endpoint ソフトウェアを実行している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 からサポートされなくなりました。

SIP アウトバウンドでは、エンドポイントを 2 つ以上の Expressway ピアに同時に登録するように設定できます。この利点は、1 つのピアとエンドポイント間の接続が切断されても、エンドポイントから他のピアへの接続が維持されることです。エンドポイントが両方のピアに同時に登録すると、エンドポイントが別のピアに登録する前に、登録の失敗を認識する間、サービスが中断することはありません。したがって、エンドポイントが到達不能になることはありません。

SIP アウトバウンドの構成はエンドポイントに固有ですが、通常は次のようになります。

- プロキシ 1
 - サーバー検出 = 手動
 - サーバーアドレス = クラスタピアの DNS 名、またはクラスタピアの IP アドレス
- プロキシ 2
 - サーバー検出 = 手動
 - サーバーアドレス = 別のクラスタピアの 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 = オン

オプション 2 – DNS SRV (第 2 選択)

このオプションを使用するには、Expressway クラスタの DNS 名に対して、各クラスタピアに等しい重みと優先順位を定義する DNS SRV レコードが利用可能である必要があります。

各 SIP エンドポイントで、SIP 設定を次のように構成します。

- サーバー検出 = 手動
- サーバーアドレス = Expressway クラスタの DNS 名

エンドポイントが DNS SRV をサポートしている場合、起動時にエンドポイントは DNS SRV リクエストを発行し、各クラスタピアに等しい重みと優先順位を定義する DNS SRV レコードを受け取ります。

その後、エンドポイントは関連するクラスタピアへの登録を試みます（優先順位/重みが考慮されます）。そのピアが利用できない場合、エンドポイントはリストされている同じ優先順位の別のピアに登録しようとします。その優先順位のすべてのピアが試行された場合は、次に低い優先順位のピアを使用します。エンドポイントが Expressway に登録できるまで、これが繰り返されます。

エンドポイントは、再登録と通話のために、登録した最初の Expressway を引き続き使用します。Expressway への接続が失われた場合、DNS SRV エントリを使用して、登録する新しい Expressway を検索し、最も優先順位の高いものから開始します。

DNS トラフィックを最小限に抑えるには、DNS SRV キャッシュ タイムアウトは、24 時間など、かなり長い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 (第 3 選択)

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 名で利用可能な DNS A レコードがなければなりません。

各 SIP エンドポイントで、SIP 設定を次のように構成します。

- サーバー検出 = 手動
- サーバーアドレス = Expressway クラスタの DNS 名

エンドポイントが DNS SRV をサポートしていない場合、スタートアップ時にエンドポイントは DNS A レコードルックアップを実行します。DNS サーバーはラウンドロビン DNS をサポートするように設定され、各クラスタピアメンバーはラウンドロビンリストで定義されます。

エンドポイントは DNS ルックアップで指定されたアドレスを取得し、関連するクラスタピアに登録しようとします。それが利用できない場合、エンドポイントは別の DNS ルックアップを実行し、指定された新しい Expressway ピアに接続しようとします。(DNS サーバーは、次のクラスタピアの IP アドレスを提供します。) エンドポイントが Expressway に登録できるまで、これが繰り返されます。

エンドポイントは、再登録と通話のために、登録した最初の Expressway を引き続き使用します。Expressway への接続が失われた場合、別の DNS ルックアップを実行して、登録する新し

オプション 4 – 静的 IP (最も優先度が低い)

い Expressway を検索します (ラウンドロビンシーケンスで Expressway を提供する DNS サーバー)。

Expressway にアクセスできない場合、エンドポイントが別の Expressway に素早く切り替わるように、DNS キャッシュタイムアウトはかなり短い時間 (たとえば、1 分以下) に設定する必要があります。

オプション 4 – 静的 IP (最も優先度が低い)

Expressway クラスタに DNS 名がない場合にこのオプションを使用します。

各 SIP エンドポイントで、SIP 設定を次のように構成します。

- サーバー検出 = 手動
- サーバーアドレス = Expressway ピアの IP アドレス

起動時に、エンドポイントは指定された IP アドレスで Expressway に登録しようとします。それが利用できない場合、エンドポイントは定期的に試行を続けます。エンドポイントが Expressway に登録できるまで、これが繰り返されます。

エンドポイントは、再登録と通話のために、登録した最初の Expressway を引き続き使用します。接続が失われた場合、再びアクセス可能になるまで、Expressway への登録を試み続けます。

H.323 エンドポイント

1 つ以上の Expressway クラスタ ピアがアクセス不能になった場合、Expressway のクラスタにエンドポイントの接続の復元性を提供するための優先順位でオプションが一覧表示されます。オプションの選択は、使用しているエンドポイントがサポートする機能によって異なります。

オプション 1 – DNS SRV (優先)

このオプションを使用するには、Expressway クラスタの DNS 名に対して、各クラスタピアに等しい重みと優先順位を定義する DNS SRV レコードが利用可能である必要があります。

各 H.323 エンドポイントで、[ゲートキーパー設定] を次のように構成します。

- 検出 = 手動
- IP アドレス = Expressway クラスタの DNS 名

エンドポイントが DNS SRV をサポートしている場合、起動時にエンドポイントは DNS SRV リクエストを発行し、各クラスタピアに等しい重みと優先順位を定義する DNS SRV レコードを受け取ります。

その後、エンドポイントは関連するクラスタピアへの登録を試みます (優先順位/重みが考慮されます)。そのピアが利用できない場合、エンドポイントはリストされている同じ優先順位の別のピアに登録するか、その優先順位のすべてのピアが試行されている場合は、次に低い (番号が高い) 優先順位のピアに登録します。

エンドポイントが Expressway に登録できるまで、これが繰り返されます。Expressway に登録する際、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」 リストで応答します。

エンドポイントは、再登録と通話のために、登録した最初の Expressway を引き続き使用します。Expressway との接続が切断された場合、提供されたリストから「代替ゲートキーパー」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限に抑えるために、かなり長い時間 (例、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 (第2選択)

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 名で利用可能な 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を次のように構成します。

- 検出 = 手動
- IP アドレス = Expressway クラスタの DNS 名

エンドポイントが DNS SRV をサポートしていない場合、スタートアップ時にエンドポイントは DNS A レコードルックアップを実行します。DNS サーバーはラウンドロビン DNS をサポートするように設定され、各クラスタピアメンバーはラウンドロビンリストで定義されます。

エンドポイントは DNS ルックアップで指定されたアドレスを取得し、関連するクラスタピアに登録しようとします。そのピアが利用できない場合、エンドポイントは別の DNS ルックアップを実行し、与えられた新しい Expressway ピアに接続しようとします。(DNS サーバーは、次のクラスタピアの IP アドレスを提供します。)

エンドポイントが Expressway に登録できるまで、これが繰り返されます。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」 リストで応答します。

エンドポイントは、再登録と通話のために、登録した最初の Expressway を引き続き使用します。接続が失われた場合、提供されたリストから「代替ゲートキーパー」を選択します。

起動時に Expressway に到達できなかった場合に、エンドポイントがすぐに別の Expressway をポイントするように、DNS キャッシュタイムアウトはかなり短い時間 (たとえば1分以下) に設定する必要があります。

オプション3 - 静的 IP (最も優先度が低い)

Expressway クラスタに DNS 名がない場合にこのオプションを使用します。

各 H.323 エンドポイントで、ゲートキーパー設定を次のように構成します。

- 検出 = 手動
- IP アドレス = Expressway ピアの IP アドレス

起動時に、エンドポイントは指定された IP アドレスで Expressway に登録しようとします。それが利用できない場合、エンドポイントは定期的に試行を続けます。

エンドポイントが Expressway に登録できるまで、これが繰り返されます。Expressway に登録する際、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」リストで応答します。

エンドポイントは、再登録と通話のために、登録した最初の Expressway を引き続き使用します。接続が失われた場合、提供されたリストから「代替ゲートキーパー」を選択します。

Expressway を Cisco TMS に追加する

Cisco TMS 管理の詳細については、ご使用のバージョンの『Cisco TelePresence Management Suite Administrator Guide』および『Cisco TelePresence Management Suite (TMS Maintenance and Operate Guide)』ページを参照してください。

Expressway 上

手順

ステップ 1 [システム > SNMP] に移動します。

- SNMP モード が v3 + Cisco TMS サポート または v2c に設定されている。
- コミュニティ名が public に設定されている。

(SNMP が以前に無効になっている場合、再起動が必要であることを示すアラームが表示される場合があります。その場合は、[メンテナンス > 再起動オプション]からシステムを再起動してください。)

ステップ 2 システム > 外部マネージャ に移動して次のことを確認します:

- アドレスが、Cisco TMS の IP アドレスまたは FQDN に設定されている。
- パスが tms/public/external/management/SystemManagementService.asmx に設定されている。
- [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 または [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 [保存 (Save)] をクリックします。

[外部マネージャ] ページの [状況] セクションに、[アクティブ] または [初期化中]¹ と表示されるはずで

す。

1

Cisco TMS 上

手順

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

ステップ 2 Expressway を配置する適切なフォルダを選択 (または作成) します (下の例では、フォルダは「クラスタ」と呼ばれています)。



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. IP アドレスまたは DNS 名でシステムを指定 (1. Specify Systems by IP addresses or DNS names)] に、Expressway の IP アドレスまたは DNS 名を入力します。

ステップ 5 [次へ (Next)] をクリックします。

ステップ 6 システムが追加されたことを示す緑色のチェックマークを見つけます。

(注)

Expressway を TMS に追加すると、TMS UI は VCS としてそれを表示します。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 [Add More Systems (Add More Systems)] をクリックします。

¹ Cisco TMS はプロトコルを HTTPS に強制する場合があります。この設定は、[管理ツール (Administrative Tools)] > [設定 (Configuration)] > [ネットワーク設定 (Network settings)] にあります。[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)] に設定されていて、[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)] に設定されている場合、プロトコルは強制的に HTTPS になります。



第 8 章

トラブルシューティング

この章では、次の項目について説明します。

- シーケンスの再起動 (51 ページ)
- レプリケーション状況の確認 (51 ページ)
- Cisco TMS での強制更新 (52 ページ)
- Expressway のアラームと警告 (52 ページ)
- Cisco TMS 警告 (55 ページ)

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常に、ピアを再起動する必要があるかどうかを確認する必要があります。特定のピアの構成を変更した場合など、1つのピアだけを再起動する必要がある場合があります。

クラスタ構成を操作している場合、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、ウェブ インターフェイス経由でアクセス可能になるのを待ちます。
2. プライマリのクラスタ複製状況とすべてのピアの状況を確認します。ピアのウェブ インターフェイスをときどき更新しながら、数分間待機します。
3. 必要に応じて、他のピアを1つずつ再起動します。毎回、アクセス可能になってから数分待ってから、レプリケーションの状態を確認します。

レプリケーション状況の確認

クラスタリングの変更を行ってから Expressway ピアが正常なステータスを報告するまで、約 5 分待つ必要がある場合があります。

1. 各ピアで [システム > クラスタリング] に移動し、クラスタデータベースのステータスが [アクティブ] としてレポートされることを確認します。

エラー ステータスがある場合、まずブラウザを更新します。それでもステータスがアクティブではない場合は、アラームを確認してください。

Cisco TMS での強制更新

Cisco TMS を使用している場合、次のように更新を強制することにより、Cisco TMS にクラスタのすべての正しい設定があることを確認します。

手順

- ステップ 1 Cisco TMS で、[Systems (システム)] > [ナビゲータ (Navigator)] に移動します。
- 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] 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 のアラームと警告

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されている場合、クラスタ名を定義する必要があります

クラスタの各 Expressway で同じクラスタ名が設定されていることを確認します。

クラスタ名は、この Expressway クラスタをアドレス指定する 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でなければなりません (例: 「cluster1.example.com」)。([クラスタ名および DNS SRV レコード \(61 ページ\)](#) を参照)。

クラスタレプリケーションエラー: (詳細) 構成の手動同期が必要です

これは:

- 「クラスタ複製エラー: 構成の手動同期が必要です」
- 「クラスタ複製エラー: 構成のプライマリ ID が一致していません。構成を手動で同期する必要があります。」
- 「クラスタレプリケーションエラー: このピアの設定がプライマリの設定と競合しています。設定を手動で同期化する必要があります。」

下位 Expressway がアラームをレポートする場合: 「クラスタレプリケーションエラー-<details>設定の同期」

下位の Expressway で、次のことを実行します。

1. SSH または他の CLI インターフェイスで `admin` としてログインします。
2. コマンドプロンプトから次のように入力します: `xcommand ForceConfigUpdate`

これにより、下位の Expressway 構成が削除され、プライマリ Expressway からの構成の更新が強制されます。



注意 プライマリ Expressway の構成が良好な状態であることがわかっている場合にのみ、このコマンドを使用します。このコマンドを実行する前にバックアップを取ることをお勧めします。

クラスタレプリケーションエラー:(詳細)ノードを再起動してください

これは次のような原因が考えられます。

「クラスタレプリケーションエラー: プライマリまたはこの下位のピア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 後もクラスタレプリケーションエラーが持続する

X8.11 では、クラスタピアごとに一意の暗号化キーを導入しました。また、ピアが間違った順序でアップグレードされた場合など、一部のアップグレードでは、下位のピアがプライマリと同期しない場合があります。この2つの問題は複雑に絡み合っており、ピアはプライマリの設定を解読できない状態に陥ります。

この現象は、下位のピアで `xcommand forceconfigupdate` を試みた後でも、クラスタレプリケーションのアラームが表示され続けることです。これは、プライマリピアで X8.11 に最近アップグレードした後である可能性があります。

常に最初にプライマリをアップグレードすることで問題を回避できますが、このエラーが繰り返される場合は、次のように解決できます。

1. プライマリピアにログインし、良好な状態であることを確認します。
2. クラスタリング設定で、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、リブートした後に、レプリケーション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、最大で 20 分後に発生する場合があります。

クラスタレプリケーションエラー: NTP サーバーに到達できません

Expressway の [システム (System)] > [時刻 (Time)] ページでアクセス可能な NTP サーバーを設定します。

クラスタレプリケーションエラー: ローカル Expressway がピアのリストに表示されません

プライマリ Expressway でこの Expressway のピアリストを確認して修正し、他のすべての Expressway ピアにコピーします (システム > クラスタリング)。

クラスタレプリケーションエラー: アップグレードが進行中のため、構成の自動レプリケーションは一時的に無効になっています

アップグレードが完了するまで待ちます。

無効なクラスタ構成です: H.323 モードをオンにする必要があります - クラスタリングはピア間の 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てください (設定 > プロトコル > H.323 を参照)。

Expressway データベースエラー: Cisco サポート担当者に連絡してください

サポート担当者が、次のステップの実行をサポートします。

1. システムのスナップショットを撮影し、サポート担当者に提供してください。
2. 次に使用してクラスタから Expressway を削除します: [クラスタからライブピアを \(永久に\) 削除する \(33 ページ\)](#)。
3. 以前にその Expressway で取ったバックアップを復元することにより、その Expressway のデータベースを復元します。
4. [クラスタにピアを追加する \(20 ページ\)](#) を使用して、Expressway をクラスタに追加し直します。

Cisco TMS 警告

Cisco TMS クラスタ診断

Cisco TMS クラスタ診断が Expressway ピアの設定の違いをレポートする場合、各 Expressway の `https://<ip address>/alternatesconfiguration.xml` の出力を比較しています。

違いを手動で確認するには、Unix / Linux システムで、各 Expressway ピアについて以下を実行します。

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

次に、diff を使用して違いを確認します。

会議ファクトリ テンプレートが複製されない

これは仕様です。会議ファクトリ%%の値はクラスタピア間で共有されません。また会議ファクトリ アプリケーション構成はクラスタ全体で複製されません。

[他の Expressway アプリケーションにおける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が繰り返し HTTPS に設定される

Cisco TMS は、接続されたシステムで特定の管理設定を強制するように構成することができます。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 は (Cisco TMS により定義された期間で) Expressway の [システム (System)]>[外部マネージャプロトコル (External Manager Protocol)]を [HTTPS] に再設定します。

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、証明書のセットアップ方法については、[Expressway を Cisco TMS に追加する \(48 ページ\)](#) を参照してください。

次の場合、Cisco TMS は 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 (On)] ([管理ツール (Administrative Tools)]> [設定 (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 (On)] ([管理ツール

(Administrative Tools)] > [設定 (Configuration)] > [ネットワーク設定 (Network Settings)]

Cisco TMS が管理設定を強制する必要がある場合は、[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 HTTPS を使用して Cisco TMS にフィードバックを提供する必要がある場合は、[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。



第 9 章

参照先

この章では、次の項目について説明します。

- [ピア固有のアイテム \(57 ページ\)](#)
- [クラスタ内 TLS ポートを保護するためのサンプルのファイアウォールルール \(60 ページ\)](#)
- [クラスタ名および DNS SRV レコード \(61 ページ\)](#)
- [隔離されたネットワークのクラスタ \(66 ページ\)](#)
- [NAPTR レコード \(67 ページ\)](#)
- [他の Expressway アプリケーションにおけるクラスタリングの影響 \(69 ページ\)](#)

ピア固有のアイテム

ほとんどの設定項目は、プライマリ ピア経由でクラスタ内のすべてのピアに適用されます。ただし、以下の項目(ウェブインタフェースで†の印)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ピア上のすべてのピアに適用される構成データを変更しないでください。せいぜいプライマリからの変更が上書きされる程度です。最悪の場合、クラスタのレプリケーションが失敗します。
-

クラスタ構成(システム>クラスタリング)

クラスタを構成する **ピアNアドレス**のリスト(ピア自身のアドレスを含む)は各ピアで指定し、それらは各ピアで同一である必要があります。

クラスタ名、**構成プライマリ**、**クラスタ IP パージョン**は各ピアで指定する必要があり、すべてのピアで同一でなければなりません。



- (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、最初に IP アドレスでクラスタを形成することをお勧めします。その後、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 > ネットワークインタフェース > イーサネット)

イーサネット速度 は各ピアに固有です。各ピアには、イーサネットスイッチへの接続に対してわずかに異なる要件があります。

IP 構成 (システム > ネットワークインタフェース > IP)

LAN 構成は各ピアに固有です。

- **IPv4 アドレス、IPv6 アドレス**、またはその両方のいずれでも、各ピアには固有の IP アドレスが必要です。
- **IP ゲートウェイ** 設定はピア固有です。各ピアは異なるゲートウェイを使用できます。

各ピアは同じプロトコルをサポートする必要があるため、IP プロトコルは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 > ネットワークインタフェース > 静的ルート)

追加するスタティックルートはピア固有であるため、必要に応じて異なるピアに異なるルートを作成できます。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には、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、クラスタ内の各ピアで異なるものでなければなりません。

DNS サーバーおよび DNS ホスト名 (システム > DNS)

DNS サーバーは各ピアに固有です。各ピアは異なる DNS サーバーのセットを使用できます。

システムのホスト名 とドメイン名 は各ピアに固有のものです。

NTP サーバーとタイムゾーン (システム > 時刻)

NTP サーバー は各ピアに固有です。各ピアは 1 つ以上の異なる NTP サーバーを使用できます。

タイムゾーン は各ピアに固有です。各ピアは異なるローカル時刻を持つことができます。

SNMP (システム > SNMP)

SNMP 設定は各ピアに固有です。それらは各ピアで異なる場合があります。

ログ記録(メンテナンス>ログ記録)

各ピアのイベントログと構成ログは、特定の Expressway のアクティビティのみをレポートします。ログレベルとリモート syslog サーバー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 サーバーをセットアップ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のアクティビティの全体像をつかむことができます。

セキュリティ証明書(メンテナンス>セキュリティ)

Expressway が使用する信頼できる CA 証明書、サーバー証明書、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)])

以下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による)
- HTTP要求を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>オプションキー)

機能をコントロールするオプション 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ためにプールされます。

各ピアには、同一の機能オプション キーのセットをインストールする必要があります。つまり、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、インストールされたライセンスの合計はクラスタ全体で使用できます。このライセンスプールビヘイビア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) 場合によっては、クラスタで使用可能なライセンスがある場合でも、ピアが必要とするライセンスを有効にするキーがないというアラームを発生させることがあります。必要なライセンスを持つ唯一のピアがサービス停止中でない限り、このカテゴリのアラームを確認し、無視できます。

Active Directory サービス ([設定 (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構成する場合、NetBIOS マシン名 (オーバーライド)、およびドメイン管理者のユーザー名とパスワードは各ピアに固有です。

会議ファクトリテンプレート ([アプリケーション (Applications)] > [会議ファクトリ (Conference Factory)])

通話を電話会議サーバーにルーティングするために、会議ファクトリアプリケーションで使用するテンプレートは、クラスタ内の各ピアに対して一意である必要があります。

クラスタ内 TLS ポートを保護するためのサンプルのファイアウォールルール

サービス拒否攻撃からクラスタピアを保護するには、Expressway の組み込みの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:

1. システム > 保護 > ファイアウォールルール > 構成に移動します。
2. 適切な IPv4 または IPv6 範囲内のすべての IP アドレスに対して、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. 優先順位の低いルールを追加します。他のピアの IP アドレスごとに 1 つずつ、これらのポートへの 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より先に実装されます。)
4. ファイアウォールルールを有効にします。

図 1: 特定のピアがこのピアのクラスタリング ポートに接続することを許可するカスタムルールを作成する

The screenshot shows the 'Firewall rules configuration' window with the 'Configuration' tab selected. The following fields are visible:

- Priority: 21
- IP address: [redacted].24
- Prefix length: 32
- Address range: [redacted].24 - [redacted].24
- Service: Custom
- Transport: TCP
- Start port: 4371
- End port: 4372
- Action: Allow
- Description: Allow TCP from peer 4

Buttons at the bottom: Create firewall rule, Cancel.

445428

図 2: 推奨される優先順位を示すルールの一覧の例

The screenshot shows the 'Firewall rules configuration' window with a list of rules. The table below represents the data shown in the screenshot:

Priority	Interface	IP address	Prefix length	Service	Transport	Start port	End port	Action	Description	Rearrange	State	Actions
10	LAN1	0.0.0.0	0	Custom	TCP	4371	4372	Drop	Block all inbound TCP to clustering ports	↓	Active	View/Edit
18	LAN1	[redacted]	32	Custom	TCP	4371	4372	Allow	Allow peer 2 inbound clustering connections	↕	Active	View/Edit
19	LAN1	[redacted]	32	Custom	TCP	4371	4372	Allow	Allow peer 3 inbound clustering connections	↑	Active	View/Edit

Buttons at the bottom: New, Delete, Undo/Redo, Select all, Unselect all, Activate firewall rules.

445426

クラスタ名および 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ことには、多くの利点があります。

- ルックアップの構造にはサービスタイプ、プロトコル、およびドメインが含まれるため、共通のドメインを使用して、異なるマシンでホストされている複数の異なるサービスを参照できます (HTTP、SIP、H.323 など)。
- DNS SRV 応答には、サーバーのプライマリ、セカンダリ、ターシャリなどのグループの指定を許可する優先順位と重みの値が含まれ、各優先順位グループ内で、重みは各サーバーを使用するアクセスの割合を定義します。

- DNS SRV 応答には複数のサーバーの優先順位と重みに関する詳細が含まれているため、受信デバイスは単一のルックアップを使用して、DNS サーバーに繰り返しクエリを行う必要なく、稼働中のサーバー (一部のサーバーがアクセス不可) を検索できます。(これは、最初のサーバーがアクセス不能であることがわかった場合に、DNS サーバーを繰り返し検索する必要があるラウンドロビン DNS の使用とは対照的です。)

DNS SRV クエリの一般的な形式は次のとおりです。

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

DNS SRV 応答は、次の形式のレコードのセットです。

- `_service._protocol.<fully.qualified.domain>. TTL クラス SRV プライオリティウェイトポートターゲット`

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 管理者ガイドおよび 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の DNS SRV 設定

このセクションでは、MRA のパブリック (外部) およびローカル (内部) DNS 要件を要約します。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](#) ページでご利用のバージョンの『Cisco Jabber プランニングガイド』を参照してください。



重要 バージョン X8.8 以降、すべての Expressway-E システムに対して正引きおよび逆引き DNS エントリを作成する必要があります。これにより、システムが TLS 接続を使用して FQDN を解決し、証明書を検証できるようになります。

パブリック DNS (外部ドメイン)

パブリック外部 DNS は、`_collab-edge._tls.<domain>` SRV レコードで設定し、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必要があります。一般的な展開には SIP サービス レコードも必要です (特に MRA 用ではありません)。たとえば、2 つの Expressway-E システムのクラスタの場合:

表 2:

ドメイン (Domain)	サービス	プロトコル	プライオリティ (Priority)	重量	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	vs1.example.com

ドメイン (Domain)	サービス	プロトコル	プライオリ ティ (Priority)	重量	ポート	ターゲット ホスト
example.com	sips	tcp	10	10	5061	vs2example.com

ローカル DNS (内部ドメイン)

ローカルの内部 DNS は `_cisco-uds._tcp.<domain>` SRV レコードで設定することを推奨しますが、X12.5 からは必須ではなくなりました。レコードの例:

表 3:

ドメイン (Domain)	サービス	プロトコル	プライオリ ティ (Priority)	重量	ポート	ターゲット ホスト
example.com	cisco-uds	tcp	10	10	8443	example.com
example.com	cisco-uds	tcp	10	10	8443	example.com

MRA で使用されるすべての Unified Communications ノードに対して、正引きと逆引きの両方のための内部 DNS レコードを作成します。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されないことを確認してください。そうしないと、Jabber クライアントは Expressway-E 経由で MRA ネゴシエーションを開始しません。

ビデオ会議のための DNS SRV 構成

Expressway で使用される sip (RFC 3263) および H.323 の DNS SRV クエリの形式は次のとおりです。

- `_sips._tcp.<fully.qualified.domain>`
- `_sip._tcp.<fully.qualified.domain>`
- `_sip._udp.<fully.qualified.domain>` - ビデオ コールでの使用はお勧めしません。音声のみのコールでのみ使用してください。
- `_h323ls._udp.<fully.qualified.domain>` - LRQ などの UDP ロケーション (RAS) シグナリング用
- `_h323cs._tcp.<fully.qualified.domain>` - H.323 コール シグナリング用

エンドポイントで通常使用される sip (RFC 3263) および H.323 の DNS SRV クエリの形式は、次のとおりです。

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

- `_sip._udp.<fully.qualified.domain>` - ビデオ コールでの使用はお勧めしません。音声のみのコールでのみ使用してください。
- `_h323ls._udp.<fully.qualified.domain>` - LRQ などの UDP ロケーション (RAS) シグナリング
- `_h323cs._tcp.<fully.qualified.domain>` - H.323 コール シグナリング
- `_h323rs._udp.<fully.qualified.domain>` - H.323 登録の場合

UDP はビデオシグナリングの転送メディアとして推奨されていません。ビデオシステムの SIP メッセージは大きすぎて、(ストリームベースではなく) データグラムベースのトランスポートで確実に伝送することはできません。

Expressway クラスタ名 ([システム (System)] > [クラスタリング (Clustering)] ページで設定) は、FQDN である必要があります。そのドメイン部分は、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 つのピアの DNS SRV レコード

引数の説明

- 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セカンダリクラスタへのフェイルオーバーを許可する異なるクラスタがある場合にのみ、異なる優先順位を使用します。その場合、プライマリクラスタピアは1つの値を持つ必要があります、他の(セカンダリ)クラスタピアはより大きい値を持つ必要があります。
 - 重みは同じである必要があります - 各ピアが均等に使用されるようにします。

DNS SRV 設定を確認する

Expressway から DNS SRV 接続を確認する

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)] > [接続テスト (Connectivity Test)] に移動します。
2. クエリする サービス記録ドメイン 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を入力します (例: _sips._tcp)。
複数のプロトコルを区切るにはカンマを使用します。例、_sip._tcp,_sips._tcp。
4. [実行 (Run)] をクリックします。

Expressway は DNS に、サービス、プロトコル、およびドメインの組み合わせで構成される SRV レコードを問い合わせます (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のデフォルト DNS サーバーにクエリを送信します (システム > DNS)。

Expressway で DNS Lookup Tool を使用する

1. [メンテナンス (Maintenance)] > [Tools (ツール)] > [ネットワークユーティリティ (Network utilities)] > [DNS ルックアップ (DNS lookup)] に移動します。
2. [ホスト (Host)] フィールドに SRV パスを入力します。
3. [ルックアップ] をクリックします。

445429

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、記載されている問題と回避策はX8.9.2での修正により無効になりました。この修正により、DNS ルックアップによって返される 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。許容される TLS（証明書が検証されない）または強制的な TLS（証明書が検証される）のオプションがあります。

後者の場合、各ピアは共通名 (CN) を DNS でルックアップする必要があり、場合によってはサブジェクト代替名 (SAN) もピアの証明書から読み取ります。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、一致する場合、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、未承諾の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、おそらくピアのプライベート IP アドレスをパブリック DNS に配置したくないでしょう。

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、問題はさらに悪化します。認証局はこれを推奨しておらず、おそらくそのような証明書は発行しません。

Expressway-E ピアにはデュアル NIC があり、スタティック NAT はありません

クラスタ ピア間で TLS を強制することができます。

1. 各ピアの DNS 構成にパブリック DNS サーバーを入力します。
2. どの LAN インターフェイスがパブリック アドレスを受け取るかを選択します。
3. パブリック DNS を構成して、各ピアの FQDN をパブリック IP アドレスに解決します。

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. クラスタ設定ページでクラスタ 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。

ピアはパブリック DNS を使用して、証明書に示されているように、互いのアイデンティティを確認します。

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のプライベート IP アドレスに加えて、NIC の 1 つにプライベートアドレスに変換されるパブリック IP アドレスを与えることができます。この場合、クラスタを形成するために FQDN を使用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 レコードが変換されたパブリック IP アドレスと一致するためです。しかし、ピアは証明書を交換するときに、互いのプライベートアドレスを見ることがになります。IP アドレス間のミスマッチは、TLS 接続の確立を妨げ、クラスタは形成されません。

クラスタを形成するには:

1. 各ピアの DNS 構成にパブリック 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スタティック NAT を有効にするかを選択します。
3. クラスタリング設定ページで他の 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、たとえば、メール、SIP、H.323 など、宛先 URI に接続するためのさまざまな方法を指定するために通常使用されます。また、これらの接続タイプで使用する優先順位を指定するためにも使用できます。たとえば、SIP TCP または SIP UDP よりも SIP TLS を優先して使用することなどです。

NAPTR レコードはまた、電話番号をダイヤル可能な URI に変換するときに、ENUM で使用されます。(ENUM の詳細については、[Expressway 導入ガイドの ENUM ダイヤル](#)を参照してください)。

NAPTR レコード形式

例: example.com への SIP アクセス、557120、557121、557122 の ENUM 検索。

```
$ 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

```

ドメイン NAPTR レコードの検索

例:NAPTR レコードにより、エンドポイントがパブリック (外部) ネットワークにいることを検出できるようになります。フラグ "s" が "se" に拡張され、"external" 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 アプリケーションにおけるクラスタリングの影響

会議ファクトリ (Multiway™)

クラスタで会議ファクトリ (Multiway) を使用する場合、次のことに注意してください。

- 会議ファクトリアプリケーション設定は、クラスタ全体で複製されません。
- 会議ファクトリテンプレートは、各 Expressway ピアで異なっている必要があります。

Multiway をサポートするためにクラスタを設定する場合:

1. 各ピアで同じ会議ファクトリエイリアス (エンドポイントが Multiway 会議を開始するために呼び出すエイリアス) をセットアップします。
2. 各ピアに別の Conference Factory テンプレートをセットアップします (各ピアが一意的な Multiway 電話会議 ID を生成するようにします)。

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 である場合、プライマリ Expressway には 775001%%@domain のテンプレート、ピア 2 には 775002%%@domain のテンプレート、ピア 3 には 775003%%@domain のテンプレートが設定されています。このように、どの Expressway が会議 ID を提供しても、他の Expressway が提供できる会議 ID を提供することはできません。

同じことがネットワーク全体に適用されます。ネットワークで会議ファクトリ機能を提供する複数の Expressway または Expressway クラスタがある場合、すべての Expressway が一意の範囲の値を提供する必要があるため、2 つの Expressway が同じ会議 ID にサービスを提供することはできません。

詳細は、[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展開ガイド](#)」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。