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」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。

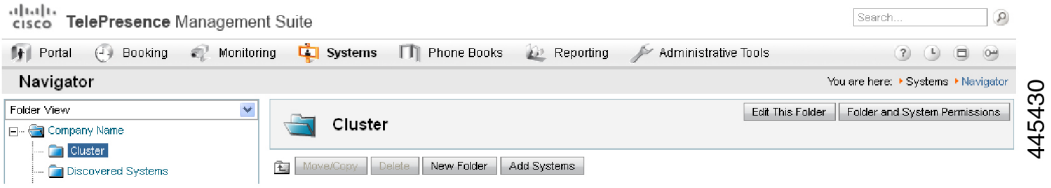
[外部マネージャ（External Manager）] ページの [ステータス（Status）] セクションの [状態（State）] が [アクティブ（Active）] または [初期化中（Initialising）] と表示されています[1]。

[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。

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。