（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、「クラスタの形成方法」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）

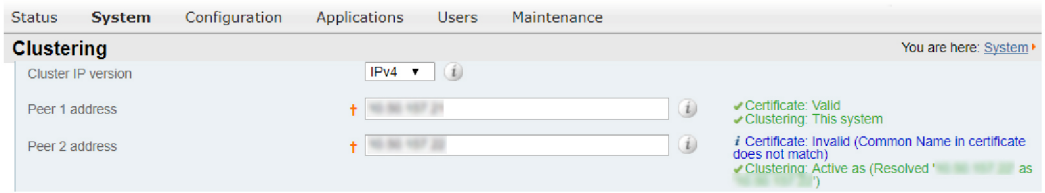
プライマリピアでマッピングを入力することを強く推奨します。アドレスマッピングは、クラスタを介して動的に複製されます。

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およびクラスタにピアを追加で説明あり）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 （1 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。

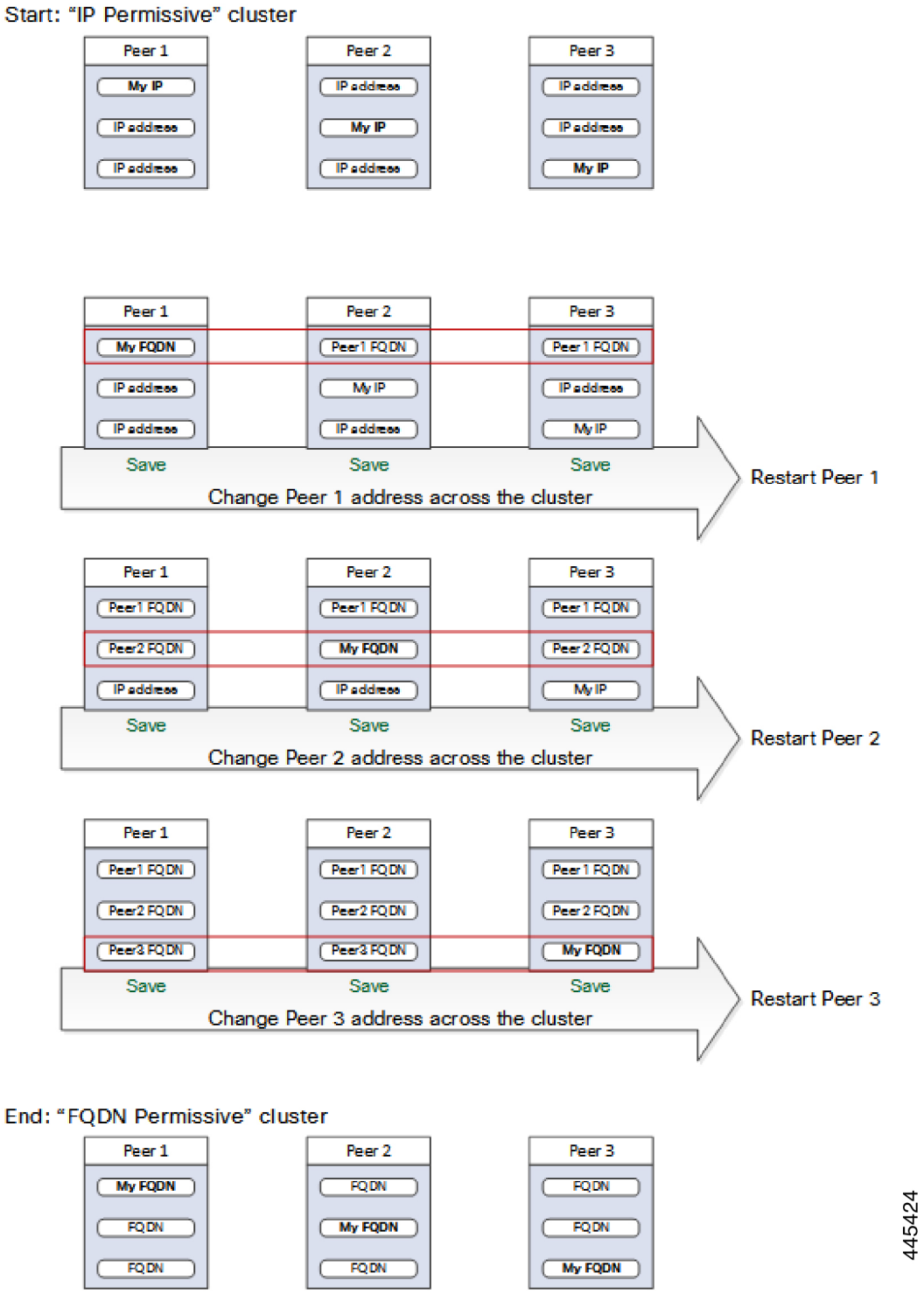
ステップ 5 一時的なクラスタリングアラームが解決するまで待機します。

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。

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。