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

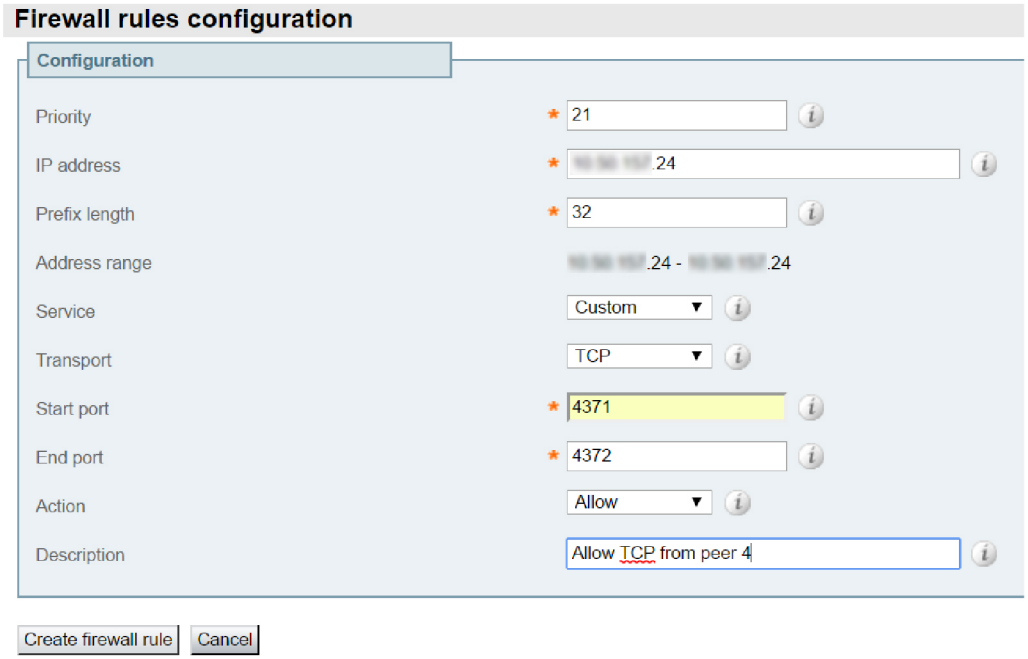
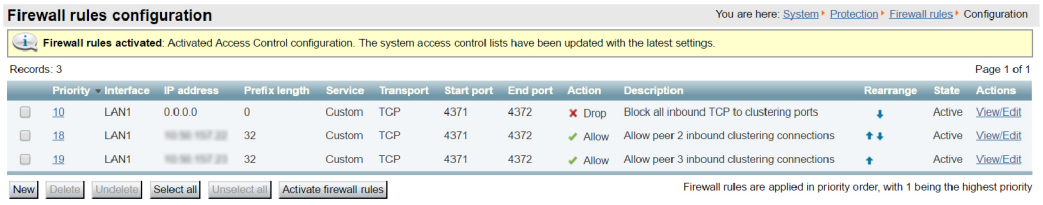


図 *2*: 推奨される優先順位を示すルールのリストの例



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 *1:*

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	vcse2.example.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 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	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`）。

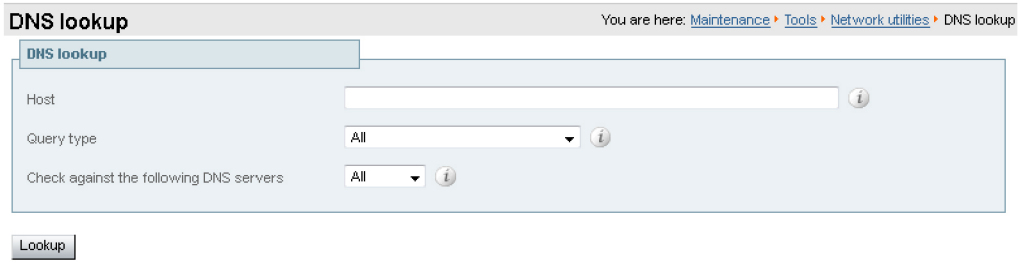
   複数のプロトコルを指定する場合は、各プロトコルをカンマで区切ります（例：`_sip._tcp`, `_sips._tcp`）。
4. [実行（Run）] をクリックします。

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。