XMPPフェデレーション用のIMandPresenceサービスの設定

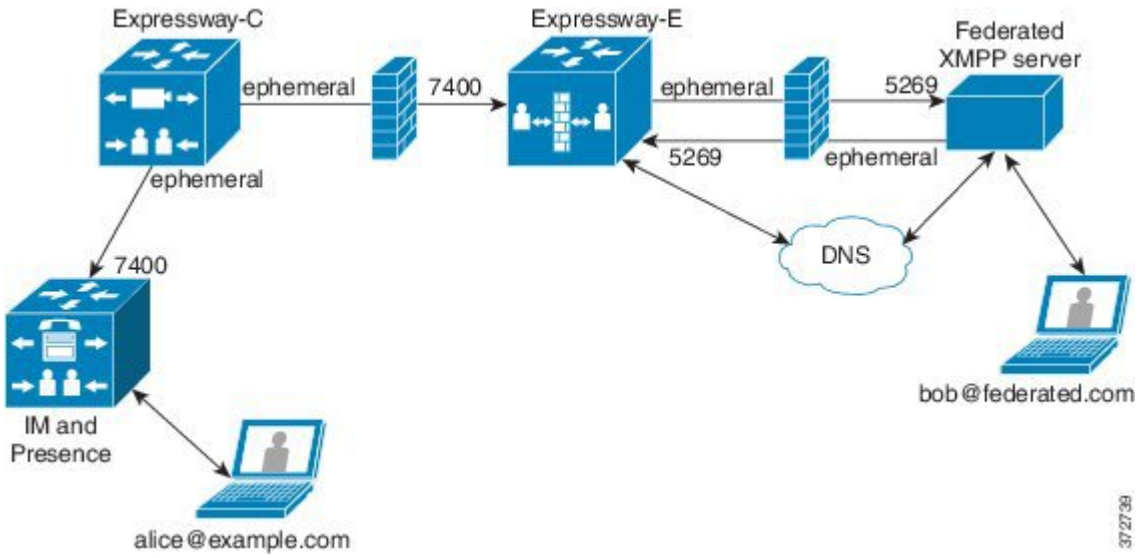
- Cisco Expressway 経由の外部 XMPP フェデレーション，1 ページ
- XMPP フェデレーションの一般的な設定を指定する，3 ページ
- XMPP フェデレーションの DNS 設定，6 ページ
- XMPP フェデレーションのポリシー設定，14 ページ
- XMPP フェデレーション用の Cisco Adaptive Security Appliance の設定，16 ページ
- XMPP フェデレーション サービスをオンにする，17 ページ

Cisco Expressway 経由の外部 XMPP フェデレーション

外部の XMPP フェデレーションを導入するための最適な方法は、Cisco Expressway 経由です。Cisco Expressway は別の XMPP の展開の Expressway-E ユーザと通信するには、IM and Presence Service に登録されたユーザをイネーブルにします。 次の図は、XMPP メッセージが Expressway-C、Expressway-E のコラボレーション エッジ ソリューションを介してオンプレミス IM and Presence Service サーバからフェデレーテッド XMPP サーバへどのように経路指定されているかを示します。 また、メッセージが DMZ ファイアウォールを通過するときに使用される接続とポートを示します。

（注） Expressway-C、Expressway-E の組み合わせはここに表示されますが、VCS Control および VCS Expressway の組み合わせを使用している場合、同じ外部の XMPP フェデレーション機能も使用できます。 Express シリーズ オプションの詳細については、『Cisco Expressway Administrator Guide (X8.2)』を参照してください。VCS オプションの詳細については、『Cisco TelePresence Video Communication Server Administrator Guide (X8.2)』を参照してください。

図 *1*：*Cisco Expressway* 経由の外部 *XMPP* フェデレーション



（注） SIP および XMPP フェデレーションは別のものであり、相互に影響を与えません。 たとえば、IM and Presence Service の SIP フェデレーションと Cisco Expressway の外部 XMPP フェデレーションを展開することができます。

サポートされるフェデレーション

Expressway-E は次の企業との XMPP フェデレーションをサポート。

- Cisco Unified Communications Manager IM and Presence Service リリース 9.1 以降
- Cisco Webex Connect Release 6.x
- XMPP 規格準拠サーバ

サポートされる展開設定

次の XMPP フェデレーションの導入オプションが使用可能。

- 外部の XMPP フェデレーションのみ（Cisco Expressway で終了）

- 内部の XMPP フェデレーションのみ（IM and Presence Service で終端）
- 内部および外部の XMPP フェデレーション（IM and Presence Service で終端）が着信接続を許可するようにファイアウォールを設定する必要があります。

Cisco Expressway 経由の外部 XMPP フェデレーションについての詳細については、『Cisco Expressway Administrator's Guide（X8.2）』を参照してください。

制約事項

- 同時内部 XMPP フェデレーションは IM and Presence Service で終端され、Cisco Expressway で終端する外部 XMPP フェデレーションはサポートされません。
- Expressway-E は（電子メールアドレスなどの）XMPP のアドレス変換をサポートしません。XMPP フェデレーションに Expressway-E を使用する場合は、IM and Presence Service からネイティブ プレゼンス Jabber ID を使用しなければなりません。

XMPP フェデレーションの一般的な設定を指定する

XMPP フェデレーションの概要

IM and Presence Service Release 9.0 以降では、次のエンタープライズとの XMPP フェデレーションをサポートしています。

- Cisco WebEx Messenger Release 7.x
- IBM Sametime Release 8.2 and 8.5
- GoogleTalk
- Cisco Unified Presence Release 8.x
- IM and Presence Release 9.x 以降

（注） IM and Presence Service は IM and Presence Service Release 9.x Enterprise と Cisco Unified Presence Release 7.x Enterprise 間の XMPP フェデレーションをサポートしていません。

IM and Presence Service と Webex Enterprise とのフェデレーションを実行する場合、Webex Connect クライアントユーザは IM and Presence Service ユーザを一時的なチャットルームや永続的なチャットルームに招待できません。 これは、WebEx Connect クライアントにある設計の制約のためです。

IM and Presence Service を XMPP でフェデレーションを実行できるようにするには、この章の手順に従って IM and Presence Service で XMPP フェデレーションを有効にし、設定する必要があります。

複数の IM and Presence Service クラスタがある場合、1 つのクラスタに少なくとも 1 つのノードで XMPP フェデレーションを有効にし、設定する必要があります。また、すべてのクラスタで XMPP フェデレーション設定を同じにする必要があります。 **トラブルシュータ診断**では、クラスタ全体の XMPP フェデレーション設定が比較され、クラスタ全体で XMPP フェデレーション設定が同じかどうかがレポートされます。

ファイアウォールのために Cisco Adaptive Security Appliance を導入する場合、次の点に注意してください。

- ルーティング、スケール、パブリック IP アドレス、および CA 権限の考慮事項については、統合の準備に関するトピックを参照してください。
- ホスト名、タイムゾーン、クロックなどの前提条件情報の設定については、Cisco Adaptive Security Appliance を設定するタスクを参照してください。

XMPP フェデレーション用サービスの再起動に関する特記事項

XMPP フェデレーションの設定のいずれかを変更する場合は、Cisco XCP ルータおよび Cisco XCP XMPP フェデレーション接続マネージャを再起動します。 サービスを再起動するには、**[IM and Presence Serviceability（IM and Presence Serviceability）]** ユーザ インターフェイスにログインします。

- Cisco XCP ルータは、[Tools（ツール）] > [Control Center - Network Services（コントロール センター - ネットワーク サービス）] を選択します。
- Cisco XCP XMPP フェデレーション接続マネージャで、[Tools（ツール）] > [Control Center - Feature Services（コントロール センター - 機能サービス）] を選択します。

Cisco XCP ルータ サービスを再起動すると、IM and Presence サービスによってすべての XCP サービスが再起動されます。

1 つのノードで XMPP フェデレーションをイネーブルまたはディセーブルにする場合、XMPP フェデレーションをイネーブルまたはディセーブルにしたノードだけでなく、クラスタ内にあるすべてのノードの Cisco XCP ルータを再起動する必要があります。 Cisco XCP ルータのその他すべての XMPP フェデレーション設定については、設定を変更したノードのみを再起動する必要があります。

ノードで XMPP フェデレーションをオンにする

デフォルトでこの設定は無効です。

手順

ステップ 1 **[Cisco Unified CM IM and Presence Administration（Cisco Unified CM IM and Presence Administration）]** ユーザ インターフェイスにログインします。 [Presence（プレゼンス）] > [Inter

Domain Federation（ドメイン間フェデレーション）] > [XMPP Federation（XMPP フェデレーション）] > [Settings（設定）]を選択します。
[XMPP Federation Node Status（XMPP フェデレーション ノード ステータス）] ドロップダウン リストで、[On（有効化）] を選択します。

ステップ 2 [Save（保存）] をクリックします。
トラブルシューティング項目

ノードで XMPP フェデレーションをイネーブルにしないと IM and Presence サービス ノードで XCP XMPP Federation Connection Manager サービスを起動できません。

次の作業

XMPP フェデレーションのセキュリティ設定の指定, （5 ページ）

XMPP フェデレーションのセキュリティ設定の指定

はじめる前に

- フェデレーション対象の外部ドメインが TLS 接続をサポートするかどうかを決定します。
- TLS および SASL 固有の設定は、SSL モードの “[TLSOptional（TLS（オプション））]” または “[TLS Required（TLS（必須））]” を選択した場合にのみ変更できます。
- TLS を使用して IM and Presence Service と IBM 間のフェデレーションを設定している場合、SSL モードの “[TLS Required（TLS（必須））]” を設定し、SASL を有効にする必要があります。

手順

ステップ 1 **Cisco Unified CM IM and Presence Administration** のユーザ インターフェイスにログインします。
[Presence（プレゼンス）] > [Inter Domain Federation（ドメイン間フェデレーション）] > [XMPP Federation（XMPP フェデレーション）] > [Settings（設定）] を選択します。

ステップ 2 ドロップダウン リストからセキュリティ モードを選択します。

a) [TLS なし（No TLS）] - IM and PresenceService で、外部ドメインとの TLS 接続が確立されません。外部ドメインとのフェデレーションには暗号化されていない接続が使用され、他のサーバの ID を識別するにはサーバダイヤルバックメカニズムが使用されます。

b) [TLS（オプション）（TLS Optional）] - IM and Presence Service で、外部ドメインとの TLS 接続の確立が試行されます。 IM and Presence Service で TLS 接続の確立に失敗すると、サーバダイヤルバックに戻り、他のサーバの ID が検証されます。

c) [TLS（必須）（TLS Required）] - 外部ドメインとのセキュア（暗号化）接続が保証されます。

ステップ 3 インストール済みのルート CA 証明書に対して外部ドメイン サーバから証明書を厳密に検証する場合は、[Require client-side security certificates（クライアント側のセキュリティ証明書が必要）]

チェックボックスをオンにします。 [TLS Optional（TLS（オプション））] または [TLS Required（TLS（必須））] のセキュリティ設定を選択すると、デフォルトでこの設定はオンです。

（注） WebEx との XMPP フェデレーションを設定している場合、[Require client-side security certificates（クライアント側のセキュリティ証明書が必要）] チェックボックスをオンにしないでください。

ステップ 4 [Enable SASL EXTERNAL on all incoming connections（すべての着信接続の SASL EXTERNAL を有効にする）] チェックボックスをオンにし、IM and Presence Service が着信接続試行の SASL EXTERNAL のサポートをアドバタイズし、SASL EXTERNAL 検証を実行します。

ステップ 5 [Enabling SASL on outbound connections（発信接続の SASL の有効化）] チェックボックスをオンにし、外部サーバが SASL EXTERNAL を要求した場合に IM and Presence Service が SASL 認証 ID を外部ドメインに送信することを確認します。

ステップ 6 IM and Presence Service への接続を試行する外部サーバの ID を検証するために DNS を使用する場合、ダイヤルバック シークレットを入力します。 IM and Presence Service は、DNS が外部サーバの ID を検証するまでは、外部サーバからのパケットを受け入れません。

ステップ 7 [Save（保存）] をクリックします。

ヒント
- セキュリティ設定の詳細については、オンライン ヘルプを参照してください。
- ノードがクラスタ間導入の一部の場合、同じセキュリティ設定を使用して各クラスタを設定する必要があります。 すべてのノードで同じ設定になるように、システム トラブルシュータを実行します。

関連トピック

ノードで XMPP フェデレーションをオンにする, （4 ページ）

XMPP フェデレーションの DNS 設定

XMPP フェデレーション用 DNS SRV レコード

IM and Presence Service で特定の XMPP フェデレーテッド ドメインを検出できるようにするには、フェデレーテッド エンタープライズからパブリック DNS サーバの _xmpp-server DNS SRV レコードを公開する必要があります。 同様に、IM and Presence Service でドメイン用に DNS と同じ DNS SRV レコードを公開する必要があります。 両方のエンタープライズはポート 5269 を公開する必要があります。 公開された FQDN は、DNS で IP アドレスに解決できる必要があります。

DNS SRV レコードは、IM and Presence Service 展開の各ドメインに公開すべきです。 **[Cisco Unified Communications Manager IM and Presence Administration（Cisco Unified Communications Manager IM and Presence Administration）]** ユーザ インターフェイスを使用して、すべてのドメインのリストを表示できます。 システム内のすべてのドメインのリストを表示するには、**[Presence Domains（プレゼンス ドメイン）]** ウィンドウに移動します。 **[Cisco Unified IM and Presence Administration**

（**Cisco Unified IM and Presence Administration**）] にログインし、[Presence（プレゼンス）] > [Domains（ドメイン）]を選択します。

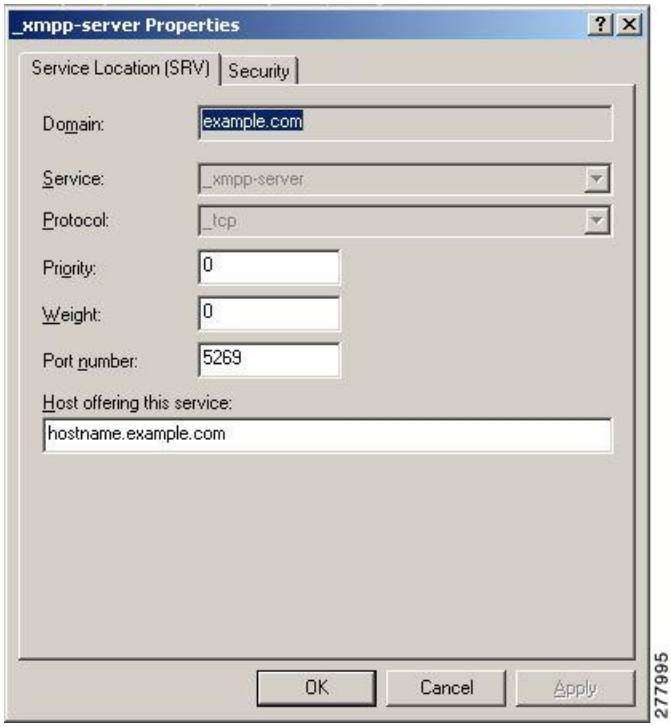
フェデレーション機能の電子メールアドレスがイネーブルの場合、**[Email Domains for Federation（フェデレーション用電子メール ドメイン）]** ウィンドウを使用して、システムのすべての電子メール ドメインのリストを見ることができます。 **[Cisco Unified IM and Presence Administration（Cisco Unified IM and Presence Administration）]** ユーザ インターフェイスにログインします。[Presence（プレゼンス）] > [Inter-Domain Federation（ドメイン間フェデレーション）] > [Email Federated Domains（電子メール フェデレーション ドメイン）] を選択します。

必要な DNS レコードは次のとおりです。

_xmpp-server._tcp.*domain*

次の図は、ドメイン **example.com** の_xmpp-server DNS SRV レコードのサンプル DNS 設定を示します。

図 *2*：*DNS SRV for _xmpp-server*



2 台の DNS レコードには、クラスタの各サーバに必要です。IPv4 用の 1 つの DNS レコードおよび IPv6 用の 2 つ目の DNS レコードが必要です。 レコードが IPv4 または IPv6 バージョンの場合は、[Host offering this service（このサービスを提供中のホスト）] フィールドで *[hostname（hostname）]* の値を使用することにより、表示してください。 次に例を示します。

- hostname-v4.example.com は DNS レコードが IPv4 バージョンであることを示します。
- hostname-v6.example.com は DNS レコードが IPv6 バージョンであることを示します。

IM and Presence Service に対するリモート ルート アクセス権がある場合、**nslookup** を実行してフェデレーテッド ドメインが検出可能かどうかを判断できます。

ヒント　DNS SRV ルックアップを実行するには、次のコマンド シーケンスを使用します。

nslookup

set type=srv

_xmpp-server._tcp.*domain*

（*domain* はフェデレーテッド エンタープライズのドメインです。）

このコマンドは、次の例のような出力を返します。「example.com」はフェデレーテッド サーバのドメインです。

```
_xmpp-server._tcp.example.com service = 0 0 5269 hostname.example.com
```

単一のクラスタの場合、クラスタ内の 1 ノードでのみ XMPP フェデレーションをイネーブルにする必要があります。 パブリック DNS でエンタープライズの 1 DNS SRV レコードを公開します。 IM and Presence Service によって、すべての着信要求は、外部ドメインからフェデレーションを実行するノードにルーティングされます。 これらの要求は、内部的には IM and Presence Service により、各ユーザにとって適切なノードにルーティングされます。 また、IM and Presence Service によって、すべての発信要求は、XMPP フェデレーションを実行するノードにルーティングされます。

（規模を拡大する場合や、）複数の IM and Presence Service クラスタをパブリッシュしたのに伴って XMPP フェデレーションを各クラスタにつき少なくとも 1 つずつ有効にする必要がある場合などには、複数の DNS SRV レコードをパブリッシュすることもできます。 XMPP フェデレーションでは、SIP フェデレーションとは異なり、IM and Presence Service が配置された企業ドメインに対してエントリ ポイントがただ 1 つである必要はありません。 そのため、IM and Presence Service は、XMPP フェデレーション用にイネーブルにするクラスタ内の公開されているノードのいずれかに対して、着信要求をルーティングできます。

クラスタ間またはマルチノード クラスタの IM and Presence Service の展開で、外部の XMPP フェデレーション ドメインが新しいセッションを開始すると、それは DNS SRV ルックアップを実行し、要求のどこにパスを指定するかを決定します。 各ドメインに対して複数の DNS SRV レコードをパブリッシュした場合、DNS ルックアップでは複数の結果が返されます。IM and Presence Service では、DNS でパブリッシュされたいずれのサーバへも、要求をルーティングすることができます。 これらの要求は、内部的には IM and Presence Service により、各ユーザにとって適切なノードにルーティングされます。 IM and Presence Service によって、発信要求は XMPP フェデレーションを実行するノードにルーティングされます。

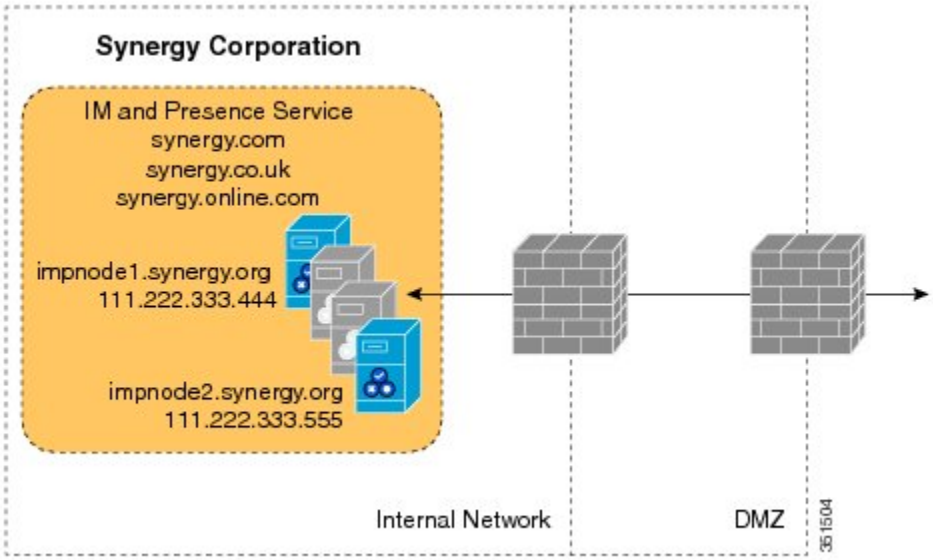
XMPP フェデレーションを実行しているノードが複数ある場合は、パブリック DNS 内でパブリッシュするノードを 1 つだけ選択することもできます。 この設定の場合、XMPP フェデレーションを実行しているノード全体に着信要求がロード バランシングされるのではなく、IM and Presence Service からその単一ノードにすべての着信要求がルーティングされます。 IM and Presence Service は、発信要求をロードバランスし、XMPP フェデレーションを実行するノードのいずれかから発信要求を送信します。

（注） 公開する DNS SRV レコードとともに、対応する DNS A および AAAA レコードを追加する必要があります。

ドメイン間フェデレーション配置の XMPP DNS SRV

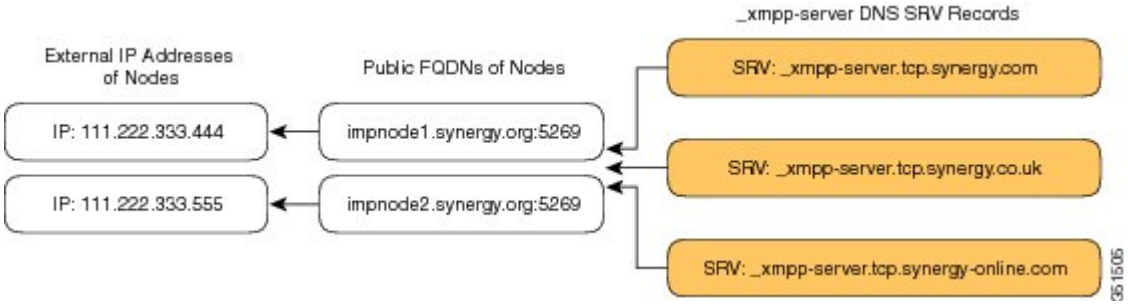
次のドメイン間フェデレーション配置の例では、2 台の IM and Presence Service ノードは XMPP フェデレーションにイネーブルになります。 DNS SRV レコードは、ホストされる IM and Presence Service 展開の各ドメインに公開しなければなりません。 次の図は、3 台のローカル ドメインとのドメイン間フェデレーション配置の例を示します。 各ドメインの_xmpp-server DNS SRV レコードを公開します。

図 *3* : *XMPP* ベースのフェデレーテッド ドメイン間配置の複数ドメイン



各 DNS SRV レコードは、XMPP フェデレーション トラフィックに指定される IM and Presence Service ノードの両方のパブリック FQDN に解決される必要があります。FQDN は IM and Presence Service ノードの外部 IP アドレスに解決される必要があります。

図 *4*：*IM and Presence Service* ノードのパブリック *FQDN* に解決される *XMPP DNS SRV*



（注） DMZ 内に配置されたファイアウォールはノードの内部 IP アドレスに IP アドレス（NAT）を変換できます。 ノードの FQDN がパブリック IP アドレスに解決できる必要があります。

関連トピック

XMPP フェデレーションのチャット機能用 DNS SRV レコード, （10 ページ）

XMPP フェデレーションのチャット機能用 DNS SRV レコード

XMPP フェデレーション配置で IM and Presence サービス ノードのチャット機能を設定するには、DNS でチャット ノード エイリアスを公開する必要があります。

チャット ノードの DNS SRV レコードを解決したホスト名は、パブリック IP アドレスに解決されます。 配置によっては、パブリック IP アドレスが 1 つの場合と、ネットワーク内のチャット ノードごとにパブリック IP アドレスが 1 つの場合があります。

表 *1*：チャット要求ルーティング

導入	チャット要求ルーティング
1 つのパブリック IP アドレス、内部的に複数のノード	XMPP フェデレーション ノードにすべてのチャット要求をルーティングしてから、チャット ノードにルーティングするには： **1** チャット ノード エイリアスの DNS SRV をポート 5269 に設定します。 **2** publicIPAddress:5269 を XMPPFederationNodePrivateIPAddress:5269 にマップする NAT コマンドを Cisco Adaptive Security Appliance または firewall\NAT サーバに設定します。

導入	チャット要求ルーティング
複数のパブリック IP アドレス、内部的に複数のノード	パブリック IP アドレスが複数ある場合、チャット要求を適切なチャット ノードに直接ルーティングできます。 1 5269 以外の任意のポート（25269 など）を使用するには、チャット ノード用の DNS SRV を設定します。 2 textChatServerPublicIPAddress:25269 を textChatServerPrivateIPAddress:5269 にマップする NAT コマンドを Cisco Adaptive Security Appliance または firewall\NAT サーバに設定します。 （注） チャット ノードで着信フェデレーション テキスト要求を処理できるようにするには、チャット ノードで Cisco XCP XMPP Federation Connection Manager をイネーブルにする必要があります。

IM and Presence サービスでチャット機能を設定する詳細については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

関連トピック

XMPP フェデレーションのチャット ノード用 DNS SRV レコードの設定, （11 ページ）

XMPP フェデレーションのチャット ノード用 DNS SRV レコードの設定

手順

ステップ 1 チャット ノードのエイリアスを取得するには：

a) **Cisco Unified CM IM and Presence Administration** のユーザ インターフェイスにログインします。 [Messaging（メッセージング）] > [Group Chat Server Alias Mapping（グループ チャット サーバ エイリアス マッピング）] を選択します。

b) [Find（検索）] を選択して、チャット ノード エイリアスのリストを表示します。

c) `conference-2.StandAloneCluster.example.com` など、DNS で公開するチャット ノード エイリアスを選択します。

ステップ 2 `example.com` ドメインのパブリック DNS サーバで、ドメイン StandAloneCluster を作成します。

ステップ 3 StandAloneClusterdomain で、conference-2domain を作成します。

ステップ 4 conference-2domain で、_tcp ドメインを作成します。

ステップ 5 _tcp ドメインで、1 つは IPv4 用、1 つは IPv6 用に 2 つの新しい DNS SRV レコードを _xmpp-server に作成します。 DNS 設定レコードの例については、次の図を参照してください。

（注） テキスト会議サーバのエイリアスが conference-2-StandAloneCluster.example.com の場合、ステップ 2 のドメインは conference-2-StandAloneCluster であり、ステップ 3 をスキップします。 ステップ 4 では、conference-2-StandAloneCluster の下に _tcp ドメインを作成します。

図 *5*：チャット機能用の *_xmpp-server* の *IPv4 DNS SRV* レコード

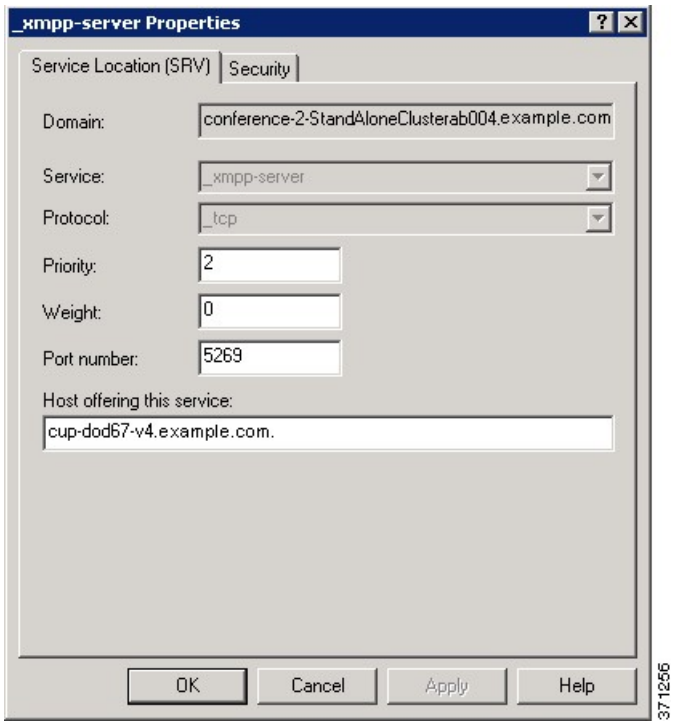


図 *6*：チャット機能用の *_xmpp-server* の *IPv6 DNS SRV* レコード

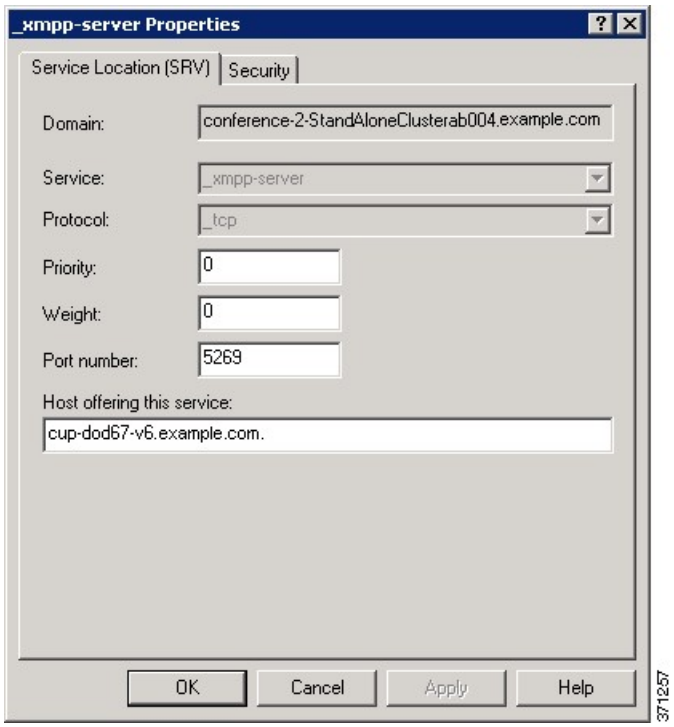
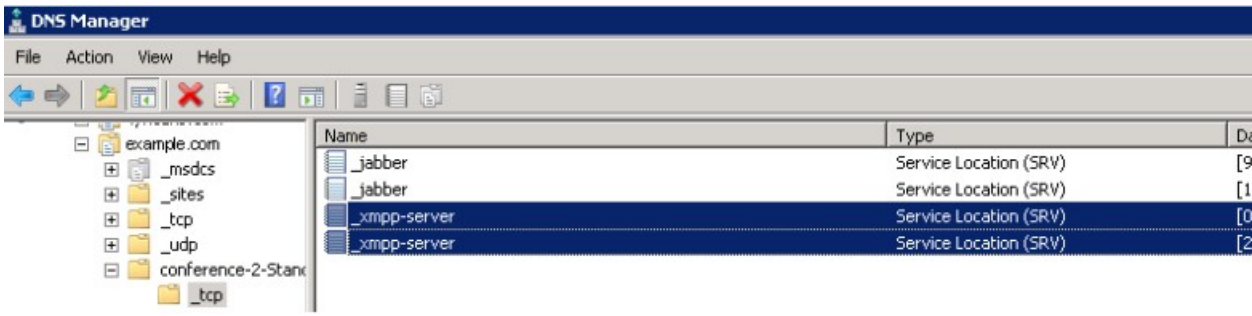


図 *7* : チャット機能用の ***DNS*** 設定



関連トピック

XMPP フェデレーション用 DNS SRV レコード, （6 ページ）

XMPP フェデレーションのポリシー設定

ポリシーの例外事項の設定

XMPP フェデレーションのデフォルト ポリシーには例外事項を設定できます。 例外事項には、例外事項を適用する外部ドメインと、その例外事項に関する方向ルールを指定する必要があります。ポリシーの例外事項のドメイン名を設定する場合は、次の点に注意してください。

- ユーザの URI または JID が `user@example.com` の場合、例外事項の外部ドメイン名を `example.com` と設定します。
- 外部エンタープライズがユーザの URI または JID に hostname.domain を使用している場合（たとえば `user@hostname.example.com` など）、例外事項の外部ドメイン名を `hostname.example.com` に設定します。
- 例外事項の外部ドメイン名にはワイルドカード（*）を使用できます。 たとえば `*.example.com` の場合、`example.com` と example.com のすべてのサブドメイン（`somewhere.example.com` など）にポリシーが適用されます。

また、IM and Presence Service がポリシーの例外事項を適用する方向も指定する必要があります。次の方向オプションを使用できます。

- [all federated packets from/to the above domain/host（上記のドメイン/ホストとの間でやり取りされるすべてのフェデレーテッド パケット）] - IM and Presence Service で、指定したドメインとの発着信トラフィックすべてを許可または拒否します。
- [only incoming federated packets from the above domain/host（上記のドメイン/ホストから着信するフェデレーテッド パケットのみ）] - IM and Presence Service は指定したドメインからの着信ブロードキャストを受信できますが、IM and Presence Service から応答は送信しません。
- [only outgoing federated packets to the above domain/host（上記のドメイン/ホストへ送信するフェデレーテッド パケットのみ）] - IM and Presence Service は指定したドメインへの送信ブロードキャストを送信できますが、IM and Presence Service から応答は受信しません。

関連トピック

XMPP フェデレーションのポリシーの設定, （15 ページ）

XMPP フェデレーションのポリシーの設定

注意 XMPP フェデレーション設定のいずれかを変更する場合、**Cisco Unified IM and Presence Serviceability** ユーザ インターフェイスの Cisco XCP ルータ（[Tools（ツール）] > [Control Center - Network Services（コントロール センタのネットワーク サービス）] を選択）、Cisco XCP XMPP Federation Connection Manager（[Tools（ツール）] > [Control Center - Feature Services（コントロール センター - 機能サービス）] を選択）でサービスを再起動する必要があります。Cisco XCP ルータ サービスを再起動すると、IM and Presence Service によってすべての XCP サービスが再起動されます。

手順

ステップ 1 **Cisco Unified CM IM and Presence Administration** のユーザ インターフェイスにログインします。[Presence（プレゼンス）] > [Inter Domain Federation（ドメイン間フェデレーション）] > [XMPP Federation（XMPP フェデレーション）] > [Policy（ポリシー）] を選択します。

ステップ 2 ドロップダウン リストからポリシー設定を選択します。

- [Allow（許可）] - IM and Presence Service は、ポリシーの例外事項の一覧で明示的に拒否したドメインを除き、XMPP フェデレーテッド ドメインからのすべてのフェデレーテッド トラフィックを許可します。
- [Deny（拒否）] - IM and Presence Service は、ポリシーの例外事項の一覧で明示的に許可したドメインを除き、XMPP フェデレーテッド ドメインからのすべてのフェデレーテッド トラフィックを拒否します。

ステップ 3 ポリシーの例外事項の一覧でドメインを設定します。

a) [Add New（新規追加）] をクリックします。
b) 外部サーバのドメイン名またはホスト名を指定します。
c) ポリシーの例外事項を適用する方向を指定します。
d) ポリシーの例外事項ウィンドウで [Save（保存）] を選択します。

ステップ 4 ポリシー ウィンドウで [Save（保存）] をクリックします。

ヒント：

フェデレーション ポリシーの推奨事項については、オンライン ヘルプを参照してください。

関連トピック

ポリシーの例外事項の設定, （14 ページ）

XMPP フェデレーション用の Cisco Adaptive Security Appliance の設定

Cisco Adaptive Security Appliance は、XMPP フェデレーションに対してファイアウォールとしてのみ機能します。 Cisco Adaptive Security Appliance 上では、着信と発信の両方の XMPP フェデレーテッド トラフィックに対してポート 5269 を開く必要があります。

次に、Cisco Adaptive Security Appliance Release 8.3 でポート 5269 を開くアクセス リストの例を示します。

ポート 5269 上で任意のアドレスから任意のアドレスへのトラフィックを許可する場合

```
access-list ALLOW-ALL extended permit tcp any any eq 5269
```

ポート 5269 上で任意のアドレスから任意のシングル ノードへのトラフィックを許可する場合

```
access-list ALLOW-ALL extended permit tcp any host private_imp_ip_address eq 5269
```

上述のアクセス リストを設定せずに、DNS で追加の XMPP フェデレーション ノードを公開する場合は、次の例のように、追加する各ノードへのアクセスを設定する必要があります。

```
object network obj_host_private_imp_ip_address
#host private_imp_ip_address
object network obj_host_private_imp2_ip_address
#host private_imp2_ip_address
object network obj_host_public_imp_ip_address
#host public_imp_ip_address
```

次の NAT コマンドを設定します。

```
nat (inside,outside) source static obj_host_private_imp1_ip obj_host_public_imp_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_5269
nat (inside,outside) source static obj_host_private_imp1_ip obj_host_public_imp_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
```

単一のパブリック IP アドレスを DNS で公開し、任意のポートを使用する場合は、次を設定します。

（この例では、追加の XMPP フェデレーション ノードが 2 つあります）

```
nat (inside,outside) source static obj_host_private_imp2_ip obj_host_public_imp_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_25269
nat (inside,outside) source static obj_host_private_imp2_ip obj_host_public_imp_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_25269
nat (inside,outside) source static obj_host_private_imp3_ip obj_host_public_imp_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_35269
```

```
nat (inside,outside) source static obj_host_private_imp3_ip obj_host_public_imp_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_35269
```

すべてがポート 5269 を使用する複数のパブリック IP アドレスを DNS で公開する場合は、次を設定します。

（この例では、追加の XMPP フェデレーション ノードが 2 つあります）

```
nat (inside,outside) source static obj_host_private_imp2_ip obj_host_public_imp2_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_5269
nat (inside,outside) source static obj_host_private_imp2_ip obj_host_public_imp2_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
nat (inside,outside) source static obj_host_private_imp3_ip obj_host_public_imp3_ip service
obj_udp_source_eq_5269 obj_udp_source_eq_5269
nat (inside,outside) source static obj_host_private_imp3_ip obj_host_public_imp_ip service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269
```

関連トピック

SIP フェデレーションに関する Cisco Adaptive Security Appliance（ASA）の設定

XMPP フェデレーション サービスをオンにする

XMPP フェデレーションを実行する各 IM and Presence サービス ノードで、Cisco XCP XMPP Federation Connection Manager サービスでオンにする必要があります。 **[Service Activation（サービス アクティベーション）]** ウィンドウから Federation Connection Manager サービスをオンにすると、IM and Presence サービスによってサービスが自動的に起動されます。**[Control Center - Feature Services（コントロール センター - 機能サービス）]** ウィンドウからサービスを手動で起動する必要はありません。

はじめる前に

Cisco Unified CM IM and Presence の管理からノードの XMPP フェデレーションをオンにします。詳細については、ノードで XMPP フェデレーションをオンにする，（4 ページ）を参照してください。

手順

ステップ 1 **[Cisco Unified IM and Presence Serviceability（Cisco Unified IM and Presence Serviceability）]** ユーザ インターフェイスにログインします。 [Tools（ツール）] > [Service Activation（サービス アクティベーション）] を選択します。

ステップ 2 [Server（サーバ）] ドロップダウン リストからサーバを選択します。

ステップ 3 [Go（実行）] をクリックします。

ステップ 4 IM and Presence サービス領域で、Cisco XCP XMPP フェデレーション接続マネージャの横にあるボタンをクリックします。

ステップ 5 [Save（保存）] をクリックします。

関連トピック

フェデレーションに関するサービスアビリティの設定