



## XMPP フェデレーション用の IM and Presence 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の指定, 3 ページ](#)
- [XMPP フェデレーション用の DNS の設定, 6 ページ](#)
- [XMPP フェデレーションのポリシー設定, 13 ページ](#)
- [XMPP フェデレーション用に Cisco Adaptive Security Appliance を設定する, 15 ページ](#)
- [XMPP フェデレーションサービスをオンにする, 16 ページ](#)

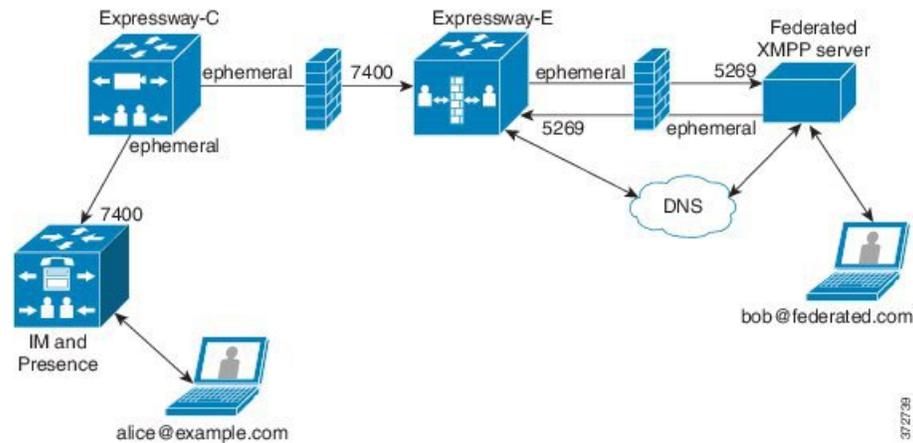
### Cisco Expressway 経由の外部 XMPP フェデレーション

外部 XMPP フェデレーションを導入するために推奨される方法は、Cisco Expressway を経由することです。Cisco Expressway は、別の XMPP 導入の Expressway-E ユーザと通信するため、IM and Presence サービス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 サービス 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を使用される接続とポートを示しています。



(注) ここでは Expressway-C と Expressway-E の組み合わせが示されていますが、VCS Control と VCS Expressway の組み合わせを使用している場合も、同じ外部 XMPP フェデレーション機能を使用できます。Expressway シリーズの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 サービスの 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します。

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

### サポートされる導入設定

次の XMPP フェデレーションの導入オプションが使用可能です。

- 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 サービスで終端)

- 内部および外部の XMPP フェデレーション (IM and Presence サービスで終端) 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

- IM and Presence サービス上で終端される同時内部 XMPP フェデレーションと Cisco Expressway 上で終端される外部 XMPP フェデレーションはサポートされません。



**重要** Cisco Expressway を通じて外部 XMPP フェデレーションを導入する場合、IM and Presence サービス上で Cisco XCP XMPP Federation Connection Manager 機能サービスをアクティブ化しないでください。

- 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 サービス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の指定

### XMPP フェデレーションの概要

IM and Presence サービスは、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ます。

- Cisco WebEx Messenger Release 7.x
- IBM Sametime Release 8.2 および 8.5
- IM and Presence リリース 9.x 以上

IM and Presence サービスと WebEx Enterprise 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 サービスユーザを一時的なチャットルームまたはパーシステント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 サービスを 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 サービスで 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 サービス 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 フェデレーション設定のいずれかを変更する場合は、Cisco XCP ルータと Cisco XCP XMPP Federation Connection Manager を再起動する必要があります。サービスを再起動するには、**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、[ツール (Tools)] > [コントロールセンター - ネットワーク サービス (Control Center - Network Services)] 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、[ツール (Tools)] > [コントロールセンター - 機能サービス (Control Center - Feature Services)] 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] ユーザ インターフェイスにログインします。[プレゼンス (Presence)] > [ドメイン間フェデレーション (Inter Domain Federation)] > [XMPP フェデレーション (XMPP Federation)] > [設定 (Settings)] を選択します。  
[XMPP フェデレーションノードのステータス (XMPP Federation Node Status)] ドロップダウンリストで、[オン (On)] を選択します。
- ステップ 2** [保存 (Save)] 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を指定する](#)、(5 ページ)

## XMPP フェデレーションのセキュリティ設定を指定する

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 “[TLS (オプション) (TLS Optional)]” または “[TLS (必須) (TLS Required)]” 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 サービスと 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 (必須) (TLS Required)]” 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。[プレゼンス (Presence)] > [ドメイン間フェデレーション (Inter Domain Federation)] > [XMPP フェデレーション (XMPP Federation)] > [設定 (Settings)] 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 Presence サービスで、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 ダイアルバック メカニズムが使用されます。
  - b) [TLS (オプション) (TLS Optional)] : IM and Presence サービスで、外部ドメインとの TLS 接続が試行されます。IM and Presence サービスで TLS 接続の確立に失敗すると、サーバ ダイアルバックに戻り、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** ルート CA 証明書に対して外部ドメインサーバの証明書を厳密に検証することを必須にするには、[クライアント側のセキュリティ証明書が必要 (Require client-side security certificates)] チェックボックスをオンにします。[TLS (オプション) (TLS Optional)] または [TLS (必須) (TLS Required)] 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、[クライアント側のセキュリティ証明書が必要 (Require client-side security certificates)] 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** [すべての着信接続の SASL EXTERNAL を有効にする (Enable SASL EXTERNAL on all incoming connections)] チェックボックスをオンにし、IM and Presence サービスが着信接続試行の SASL EXTERNAL のサポートをアダプタイズし、SASL EXTERNAL 検証を実行します。
- ステップ 5** 外部サーバが SASL EXTERNAL を要求する場合に、IM and Presence サービスによって SASL 認証 ID が外部ドメインに確実に送信されるようにするには、[アウトバウンド接続で SASL を有効化 (Enabling SASL on outbound connections)] チェックボックスをオンにします。
- ステップ 6** IM and Presence サービス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 サービスは、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** [保存 (Save)] 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。
  - サーバ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 フェデレーション用の DNS の設定

### XMPP フェデレーション用 DNS SRV レコード

IM and Presence サービスで特定の 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 サービスでドメイン用に 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 サービス導入環境内の各ドメインに対して公開する必要があります。[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、[プレゼンス ドメイン (Presence Domains)] ウィンドウに移動します。[Cisco Unified IM and Presence Administration] にログインし、[プレゼンス (Presence)] > [ドメイン (Domains)] を選択します。

フェデレーション機能の電子メール アドレスが有効な場合は、[フェデレーション用電子メール ドメイン (Email Domains for Federation)] ウィンドウを使用して、システム内のすべてのメール ドメインのリストを表示することもできます。[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。[プレゼンス (Presence)] > [ドメイン間フェデレーショ

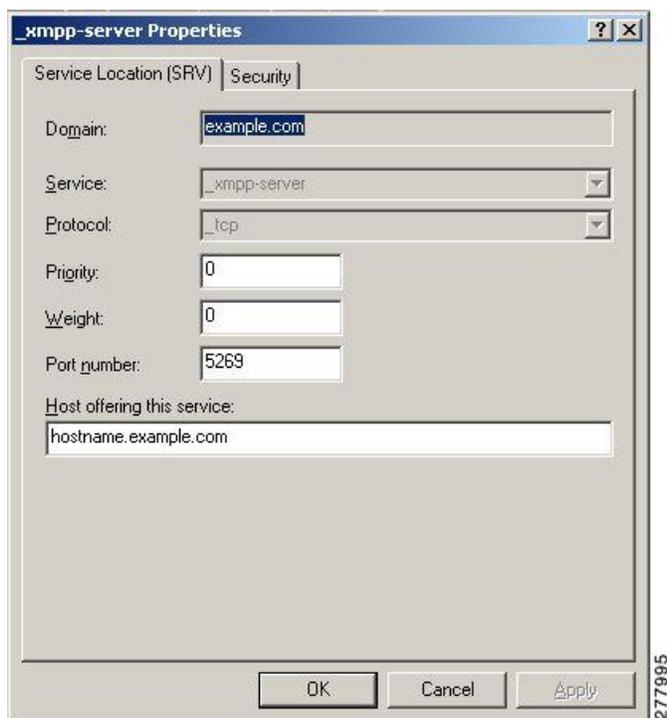
ン (Inter-Domain Federation) ]>[電子メールフェデレーションドメイン (Email Federated Domains) ]  
を選択します。

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 DNS 設定例を示しています。

図 2 : “\_xmpp-server”の DNS SRV



クラスターではサーバごとに 2 つの DNS レコードが必要です。つまり、IPv4 用の DNS レコードが 1 つに IPv6 用の DNS レコードがもう 1 つです。レコードが IPv4 または IPv6 バージョンの場合は、[このサービスを提供中のホスト (Host offering this service) ] フィールドで *[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 サービス 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 サービスによって、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 サービスにより、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 サービスによって、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 サービス 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 サービス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 サービスは、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。

クラスタ間およびマルチノードクラスタ IM and Presence サービス展開では、外部 XMPP フェデレーテッドドメインが新しいセッションを開始すると、要求をルーティングする場所を設定するために DNS SRV ルックアップが実行されます。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 サービスでは、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 サービスにより、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 サービスによって、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 サービス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 サービスは、発信要求をロードバランシングし、XMPP フェデレーションを実行するノードからの発信要求を送信します。

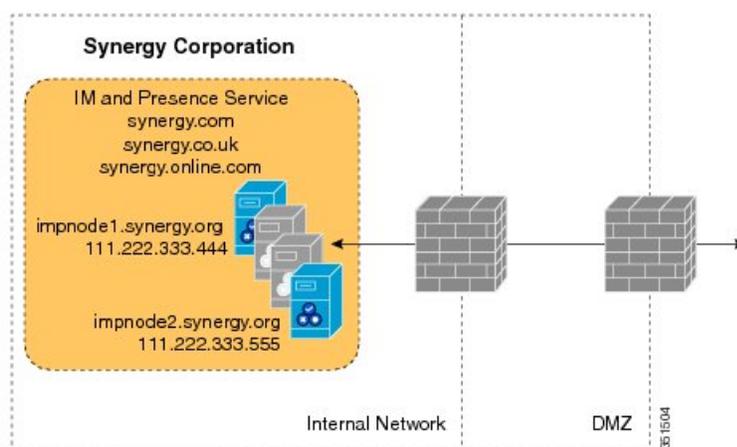


(注) 公開する DNS SRV レコードとともに、対応する DNS A および AAAA レコードを追加する必要があります。

### ドメイン間フェデレーション配置の XMPP DNS SRV

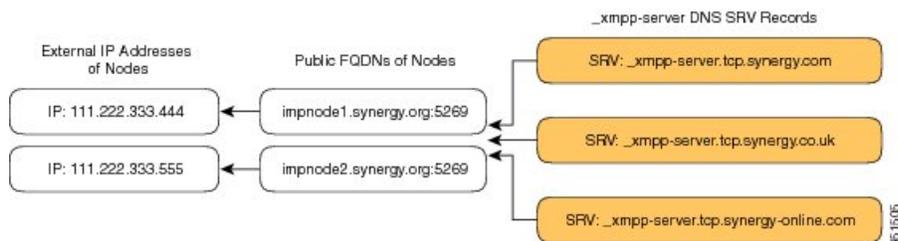
次の例のドメイン間フェデレーション導入では、2つの IM and Presence サービス ノードが XMPP フェデレーション用に有効になります。DNS SRV レコードは、IM and Presence サービス導入環境でホストされる各ドメインに対して公開する必要があります。次の図は、3つのローカルドメインが存在するドメイン間フェデレーション導入の例を示しています。ドメインごとに、\_xmpp-server DNS SRV レコードを公開する必要があります。

図 3: *Interdomain* の XMPP ベースの連合環境複数ドメイン



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 サービス 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 サービス 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 サービス 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 フェデレーション導入環境で 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。導入環境によっては、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: チャット要求のルーティング

展開	チャット要求のルーティング
1 つのパブリック IP アドレス、内部的に複数のノード	<p>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、次の手順を実行します。</p> <ol style="list-style-type: none"> <li>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。</li> <li>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。</li> </ol>
複数のパブリック IP アドレス、内部的に複数のノード	<p>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。</p> <ol style="list-style-type: none"> <li>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。</li> <li>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。</li> </ol> <p>(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 XMPP Federation Connection Manager を有効にする必要があります。</p>

IM and Presence サービスでチャット機能を設定する方法については、『*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** チャットノードエイリアスを取得するには、次の手順を実行します。
- [Cisco Unified CM IM and Presence Administration] ユーザーインターフェイスにログインします。  
[メッセージング (Messaging)] > [グループチャットサーバエイリアスのマッピング (Group Chat Server Alias Mapping)] を選択します。
  - [検索 (Find)] をクリックして、チャットノードエイリアスのリストを表示します。
  - 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** StandAloneCluster ドメインで、conference-2 ドメインを作成します。
- ステップ 4** conference-2 ドメインで、\_tcp ドメインを作成します。
- ステップ 5** \_tcp ドメインで、\_xmpp-server 用の 2 つの新しい DNS SRV レコードを作成します。1 つは IPv4 用、もう 1 つは IPv6 用です。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) 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、手順 2 のドメインは conference-2-StandAloneCluster であり、手順 3 をスキップします。手順 4 で、conference-2-StandAloneCluster に \_tcp ドメインを作成します。

図 5：チャット機能の\_xmpp-server の IPv4 DNS SRV レコード

The screenshot shows the 'xmpp-server Properties' dialog box with the 'Service Location (SRV)' tab selected. The fields are as follows:

- Domain: conference-2-StandAloneClusterab004.example.com
- Service: \_xmpp-server
- Protocol: \_tcp
- Priority: 2
- Weight: 0
- Port number: 5269
- Host offering this service: cup-dod67-v4.example.com

Buttons at the bottom: OK, Cancel, Apply, Help.

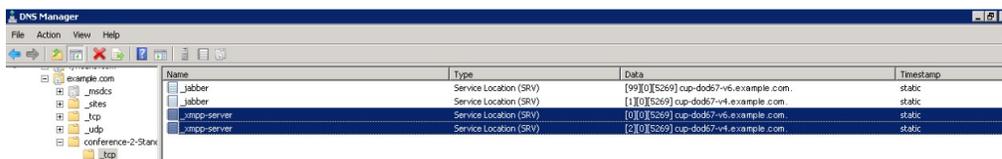
図 6：チャット機能の\_xmpp-server の IPv6 DNS SRV レコード

The screenshot shows the 'xmpp-server Properties' dialog box with the 'Service Location (SRV)' tab selected. The fields are as follows:

- Domain: conference-2-StandAloneClusterab004.example.com
- Service: \_xmpp-server
- Protocol: \_tcp
- Priority: 0
- Weight: 0
- Port number: 5269
- Host offering this service: cup-dod67-v6.example.com

Buttons at the bottom: OK, Cancel, Apply, Help.

図 7：チャット機能用の DNS 設定



Name	Type	Data	Timestamp
_jabber	Service Location (SRV)	[99]0[5269]cup-d0d57-v6.example.com.	static
_jabber	Service Location (SRV)	[17]0[5269]cup-d0d57-v4.example.com.	static
_xmpp-server	Service Location (SRV)	[01]0[5269]cup-d0d57-v6.example.com.	static
_xmpp-server	Service Location (SRV)	[21]0[5269]cup-d0d57-v4.example.com.	static

371255

## 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 サービス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。

- [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 (all federated packets from/to the above domain/host) ] - IM and Presence サービスで、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。
- [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 (Only incoming federated packets from the above domain/host) ] - IM and Presence サービス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 サービスから応答は送信しません。
- [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 (only outgoing federated packets to the above domain/host) ] - IM and Presence サービス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 サービス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を設定する, \(14 ページ\)](#)

## XMPP フェデレーションのポリシーを設定する

**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 ([ツール (Tools)] > [コントロールセンターのネットワーク サービス (Control Center - Network Services)] を選択)、Cisco XCP XMPP Federation Connection Manager ([ツール (Tools)] > [コントロールセンター - 機能サービス (Control Center - Feature Services)] 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 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。

**手順**

- ステップ 1** [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。[プレゼンス (Presence)] > [ドメイン間フェデレーション (Inter Domain Federation)] > [XMPP フェデレーション (XMPP Federation)] > [ポリシー (Policy)] を選択します。
- ステップ 2** ドロップダウンリストから次のポリシー設定を選択します。
- [許可 (Allow)] - IM and Presence サービスは、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。
  - [拒否 (Deny)] - IM and Presence サービスは、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するには、次の手順を実行します。
- a) [新規追加 (Add New)] 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 [保存 (Save)] をクリックします。
- ステップ 4** ポリシー ウィンドウで [保存 (Save)] 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, \(13 ページ\)](#)

## XMPP フェデレーション用に Cisco Adaptive Security Appliance を設定する

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、リリース 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。[サービス アクティベーション (Service Activation)] 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。[コントロールセンター - 機能サービス (Control Center - Feature Services)] 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

Unified CM IM and Presence Administration 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] ユーザ インターフェイスにログインします。[ツール (Tools) ]>[サービス アクティベーション (Service Activation) ] を選択します。
  - ステップ 2 [サーバ (Server) ] 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 [移動 (Go) ] をクリックします。
  - ステップ 4 [IM and Presence サービス (IM and Presence Services) ] エリアで、Cisco XCP XMPP Federation Connection Manager サービスの横にあるボタンをクリックします。
  - ステップ 5 [保存 (Save) ] 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](#)

