XMPP フェデレーションの IM および Presence サービス構成

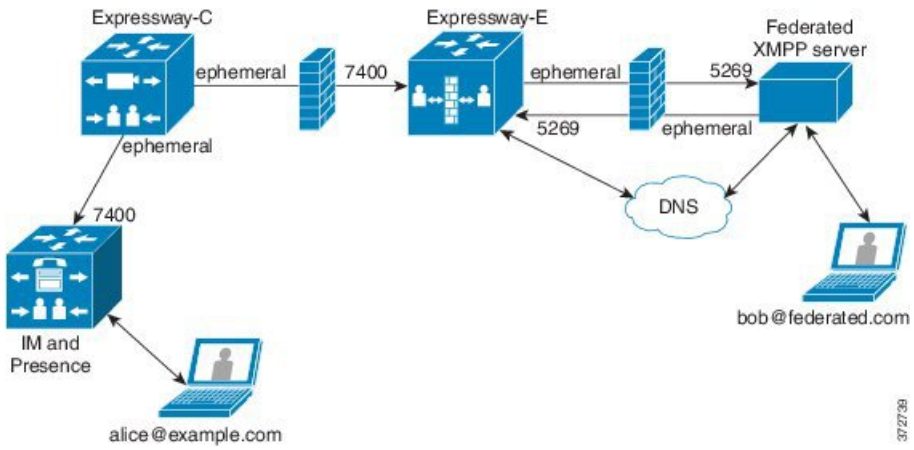
このセクションでは、XMPP フェデレーションの IM and Presence サービスの設定について説明します。

External XMPP Federation through Cisco Expressway

The preferred method for deploying external XMPP federation is through Cisco Expressway. Cisco Expressway enables users registered to IM and Presence Service to communicate via the Expressway-E with users from a different XMPP deployment. The following diagram shows how XMPP messages are routed from an on-premises IM and Presence Service server via the Expressway-C and Expressway-E Collaboration Edge solution to the federated XMPP server. It also shows the ports and connections that are used as the messages traverse DMZ firewalls.

Note The Expressway-C and Expressway-E combination is shown here, however the same external XMPP federation functionality is also available when using a VCS Control and VCS Expressway combination. Refer to Cisco Expressway Administrator Guide (X8.2) for more information about the Expressway series option or Cisco TelePresence Video Communication Server Administrator Guide (X8.2) for more information about the VCS option.

Figure 1: External XMPP Federation through Cisco Expressway



Note SIP and XMPP federations are separate and do not impact each other. For example, it is possible to deploy SIP federation on IM and Presence Service and external XMPP federation on Cisco Expressway.

Supported Federations

Expressway-E supports XMPP federation with the following enterprises:

- Cisco Unified Communications Manager IM and Presence Service Release 9.1 or later
- Cisco WebEx Connect Release 6.x
- XMPP standards-compliant servers

Supported Deployment Configurations

The following XMPP federation deployment options are available:

- external XMPP federation only (terminated on Cisco Expressway)
- internal XMPP federation only (terminated on IM and Presence Service)
- internal and external XMPP federation (terminated on IM and Presence Service) but requires you to configure your firewall to allow inbound connections.

For more information about external XMPP federation through Cisco Expressway, see Cisco Expressway Administrator Guide (X8.2)

Restrictions

- Simultaneous internal XMPP federation terminated on IM and Presence Service and external XMPP federation terminated on Cisco Expressway is not supported.

Important If you deploy external XMPP federation through Cisco Expressway, do not activate the Cisco XCP XMPP Federation Connection Manager feature service on IM and Presence Service.

- Expressway-E does not support XMPP address translation (of email addresses, for example). If you are using Expressway-E for XMPP federation, you must use native presence Jabber IDs from IM and Presence Service.

XMPP フェデレーションの全般設定の構成

このセクションでは、XMPP フェデレーションの一般設定を行う方法について説明します。

XMPP フェデレーションの概要

IM and Presence Service では、以下の企業の XMPP フェデレーションをサポートします。

- Cisco Webex Messenger リリース 7.x
- IBM Sametime リリース 8.2 および 8.5
- IM and Presence リリース 9.x 以降

IM and Presence Service が Webex Enterprise とフェデレートしている場合、Webex Connect クライアント ユーザーは、 IM and Presence Service ユーザーを一時的または永続的なチャットルームに招待することはできません。これは、WebEx Connect クライアントの設計上の制約によるものです。

IM and Presence Service が XMPP を介してフェデレーションできるようにするには、この章で説明する手順に従って、 IM and Presence Serviceで XMPP フェデレーションを有効にして構成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は、クラスタごとに少なくとも 1 つのノードでXMPPフェデレーションを有効にして構成する必要があります。XMPPフェデレーション構成は、クラスタ間で同一である必要があります。**診断トラブルシューター**は、クラスタ間でXMPPフェデレーション構成を比較し、XMPPフェデレーション構成がクラスタ間で同一でない場合に報告します。

ファイアウォールの目的でCisco適応型セキュリティアプライアンスを展開する場合は、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 権限に関する考慮事項については、統合の準備に関連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構成については、Cisco 適応型セキュリティ アプライアンス を構成するタスクを参照してください。

XMPP フェデレーションのサービスの再起動に関する重要事項

XMPP フェデレーションの設定を変更した場合は、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** ユーザー インターフェイスにログインします。

- Cisco XCP ルータで、**[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 Federation Connection Manager で、[ツール（ **Tools**） > **] [コントロール センター（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 Service によりすべての XCP サービスが再起動されます。

ノードでXMPPフェデレーションを有効または無効にする場合は、XMPPフェデレーションが有効または無効になっているノードだけでなく、クラスタ内のすべてのノードで Cisco XCP ルータを再起動する必要があります。他のすべてのXMPPフェデレーション設定の場合、Cisco XCP ルータの再起動は、設定を変更するノードでのみ必要です。

ノードでの XMPP フェデレーションの有効化

デフォルトでこの設定は無効です。

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（Interdomain 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 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オンにしない限り、 IM and Presence Service ノードで XCP XMPP Federation Connection Manager サービスを開始できません。

次の作業：

XMPP フェデレーションのセキュリティ設定の構成

XMPP フェデレーションのセキュリティ設定の構成

始める前に

- フェデレーションしている外部ドメインが TLS 接続をサポートしているかどうかを確認します。
- 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構成できます。
- TLS を使用して IM and Presence Service と IBM 間のフェデレーションを構成する場合は、SSL モード 「TLS Required」を構成し、SASL を有効にする必要があります。

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（Interdomain 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 Service は外部ドメインとの TLS 接続を確立しません。システムは、暗号化されていない接続を使用して外部 DOMIM and Presence Service ain とフェデレーションし、サーバー ダイヤルバック メカニズムを使用して他のサーバーの ID を確認します。

b) TLS オプション：外部ドメインとの TLS 接続の確立を試行します。 IM and Presence Service が TLS 接続の確立に失敗した場合、サーバー ダイヤルバックに戻り、他のサーバーの ID を確認します。

c) [必須の TLS（TLS Required）] : システムは、外部ドメインとのセキュアな（暗号化された）接続を保証します。

ステップ 3 インストールされたルート CA 証明書に対して外部ドメイン サーバからの証明書を厳密に検証する場合は、**[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）] セキュリティ設定を選択した場合、この設定はデフォルトでオンになります。

（注） Webex で XMPP フェデレーションを構成する場合は、**[クライアント側のセキュリティ証明書を要求する（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 **[すべての着信接続で 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て、 IM and Presence Service が着信接続試行で SASL EXTERNAL のサポートをアドバタイズし、SASL EXTERNAL 検証を実装するようにします。

ステップ 5 **[発信接続で SASL を有効にする（Enabling SASL on outbound connections）]** チェックボックスをオンにして、外部サーバーが SASL EXTERNAL を要求した場合に IM and Presence Service が外部ドメインに SASL 認証 ID を送信するようにします。

ステップ 6 IM and Presence Serviceに接続しようとしている外部サーバーの ID を確認するために DNS を使用する場合は、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、外部サーバー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
- セキュリティ設定に関する詳細は、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展開の一部である場合は、各クラスタに同じセキュリティ設定を構成する必要があります。システム トラブルシュータを実行して、構成がすべてのノードで一貫していることを確認します。

関連情報

ノードでの XMPP フェデレーションの有効化

XMPP フェデレーションの DNS 構成

ここでは、XMPP フェデレーションの DNS 構成の概要について説明します。

XMPP フェデレーションの DNS SRV レコード

IM and Presence Service が特定の 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 エンタープライズがパブリック DNS サーバーで _xmpp-server DNS SRV レコードを発行する必要があります。同様に、IM and Presence Service は、そのドメインの DNS で同じ DNS SRV レコードを発行する必要があります。両方のエンタープライズがポート 5269 を発行する必要がある。発行された FQDN は、DNS の IP アドレスに解決できる必要もあります。

IM and Presence Service 展開内のドメインごとに、DNS SRV レコードを発行する必要があります。**Cisco Unified Communications Manager IM and Presence Administration** ユーザー 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。**[プレゼンス ドメイン（Presence Domains）]** ウィンドウに移動して、システム内のすべてのドメインのリストを表示します。**[Cisco Unified CM 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。

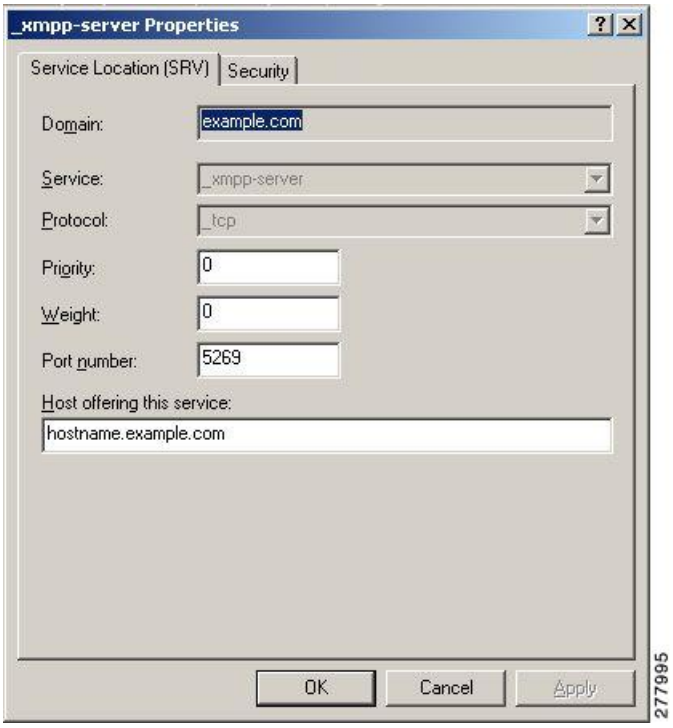
フェデレーション機能の電子メール アドレスが有効になっている場合は、**[フェデレーションの電子メール ドメイン（Email Domains for Federation）]** ウィンドウを使用して、システム内のすべての電子メール ドメインのリストを表示することもできます。**Cisco Unified CM IM and Presence Administration** のユーザー インターフェイスにログインします。**[プレゼンス（Presence）] > [ドメイン間フェデレーション（Inter-Domain Federation）] > [電子メール フェデレーテッド ドメイン（Email 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*

次の図に、ドメイン **example.com**の _xmpp-server DNS SRV レコードの DNS 設定の例を示します。

図 *2 : _xmpp-server* の *DNS SRV*



クラスタ内のサーバーごとに 2 つの DNS レコードが必要です。1 つは IPv4 用の DNS レコード、もう 1 つは IPv6 用の DNS レコードです。**[このサービスを提供するホスト（Host Offering this service）]** フィールドの ホスト名（*hostname*） の値を使用して、レコードが IPv4 または IPv6 バージョンであるかどうかを示します。例 :

- **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 へのリモート ルート アクセスがある場合は、 **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確認できます。

ヒント DNS SRV ルックアップを実行するには、次の一連のコマンドを使用します。

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。）

このコマンドにより、次の例のような出力が返されます。ここで、「example.com」はフェデレーテッド サーバーのドメインです。

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

単一クラスタの場合、クラスタ内の1つのノードでXMPPフェデレーションのみを有効にする必要があります。パブリック DNS で企業の 1 つの DNS SRV レコードを発行します。IM and Presence Service は、外部ドメインからのすべての着信要求を、フェデレーションを実行しているノードにルーティングします。内部的には、IM and Presence Service が要求をユーザの正しいノードに再ルーティングします。また、 IM and Presence Service は、XMPP フェデレーションを実行しているノードにすべての発信要求をルーティングします。

また、複数の DNS SRV レコードを発行することもできます（スケール目的など）。または、複数の IM and Presence Service クラスタがあり、クラスタごとに少なくとも 1 回は XMPP フェデレーションを有効にする必要があります。SIP フェデレーションとは異なり、XMPP フェデレーションでは、 IM and Presence Service エンタープライズ ドメインの単一のエントリ ポイントは必要ありません。その結果、 IM and Presence Service は、XMPP フェデレーションを有効にしたクラスタ内で発行されたノードのいずれかに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 Service 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、DNS SRV ルックアップを実行して要求のルーティング先を決定します。ドメインごとに複数の DNS SRV レコードを発行すると、DNS ルックアップは複数の結果を返します。 IM and Presence Service は、DNS が発行する任意のサーバに要求をルーティングできます。内部的には、 IM and Presence Service が要求をユーザの正しいノードに再ルーティングします。IM and Presence Service は、XMPP フェデレーションを実行しているノードのいずれかに発信要求をルーティングします。

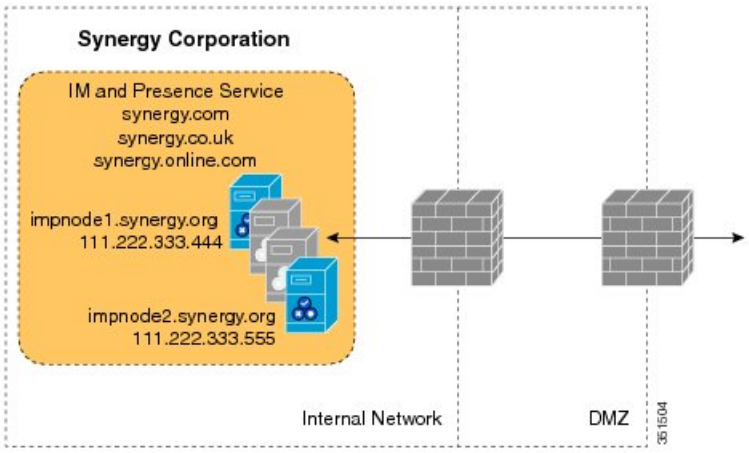
XMPP フェデレーションを実行している複数のノードがある場合でも、パブリック DNS で 1 つのノードのみを発行することを選択できます。この設定では、 IM and Presence Service は、XMPP フェデレーションを実行しているノード間で着信要求をロードバランシングするのではなく、すべての着信要求を単一のノードにルーティングします。IM and Presence Service は発信要求をロードバランシングし、XMPP フェデレーションを実行しているノードのいずれかから発信要求を送信します。

（注） 発行する DNS SRV レコードとともに、対応する DNS A および AAAA レコードも追加する必要があります。

ドメイン間フェデレーション展開での XMPP DNS SRV

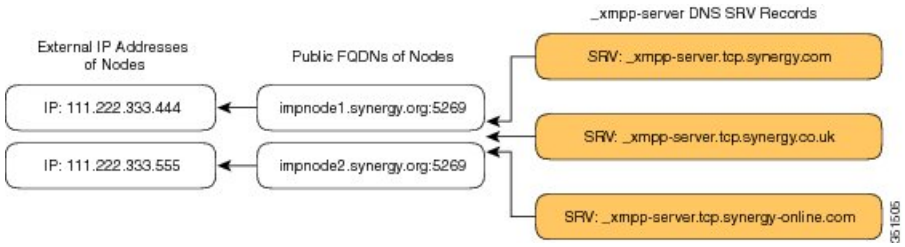
次のドメイン間フェデレーション展開の例では、2 つの IM and Presence Service ノードで XMPP フェデレーションが有効になっています。IM and Presence Service 展開でホストされているドメインごとに、DNS SRV レコードを発行する必要があります。次の図は、3 つのローカルドメインを使用したドメイン間フェデレーション展開の例を示しています。ドメインごとに_xmpp-server DNS SRV レコードを発行する必要があります。

図 *3 : XMPP* ベースのフェデレーテッド ドメイン間展開での複数のドメイン



各 DNS SRV レコードは、XMPP フェデレーテッド トラフィック用に指定された IM and Presence Service ノードの両方のパブリック FQDN に解決する必要があり、FQDN は IM and Presence Service ノードの外部 IP アドレスに解決する必要があります。

図 *4 : IM and Presence* サービス ノードのパブリック *FQDN* への *XMPP DNS SRV* の解決



（注） DMZ 内に展開されたファイアウォールは、IP アドレス（NAT）をノードの内部 IP アドレスに変換できます。ノードの FQDN は、パブリック IP アドレスにパブリックに解決可能である必要があります。

関連情報 -

XMPP フェデレーションのチャット機能の DNS SRV レコード

XMPP フェデレーションのチャット機能の DNS SRV レコード

XMPP フェデレーション展開の IM and Presence Service ノードでチャット機能を構成する場合は、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 レコードが解決するホスト名は、パブリック IP アドレスに解決されます。展開に応じて、ネットワーク内のチャットノードごとに単一のパブリック IP アドレスまたはパブリック IP アドレスを使用できます。

表 *1:* チャット リクエスト ルーティング

デプロイ	チャット リクエスト ルーティング
単一のパブリック IP アドレス、内部に複数のノード	すべてのチャット要求を XMPP フェデレーション ノードに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。 **1.** チャット ノード エイリアスの DNS SRV がポート 5269 を指すように構成定します。 **2.** publicIPAddress:5269 を XMPPFederationNodePrivateIPAddress:5269 にマッピングする Cisco 適応型セキュリティ アプライアンス または firewall\NAT サーバで構成された NAT コマンドを構成します。
複数のパブリック IP アドレス、内部に複数のノード	複数のパブリック IP アドレスがある場合は、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することを選択できます。 **1.** 5269 以外の任意のポート（25269 など）を使用するようにチャット ノードの DNS SRV を構成します。 **2.** Cisco 適応型セキュリティ アプライアンス または firewall\NAT サーバで、textChatServerPublicIPAddress:25269 を textChatServerPrivateIPAddress:5269 にマッピングする NAT コマンドを構成します。 （注） チャット ノードが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 をオンにする必要があります。

IM and Presence Service のチャット機能構成に関する詳細は、『*Cisco Unified Communications Maanger*』記載の「*IM and Presence Service*」の構成および管理を参照してください。

関連情報 -

XMPP フェデレーションのチャット機能の DNS SRV レコード

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

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、次の手順を実行します。

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。**[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。

b) **[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。

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

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

ステップ 3 StandAloneClusterdomain 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 用に 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 構成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、手順 2 のドメインは Conference-2-StandAloneCluster であるため、手順 3 をスキップします。手順 4 で、conference-2-StandAloneCluster の下に _tcp ドメインを作成します。

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

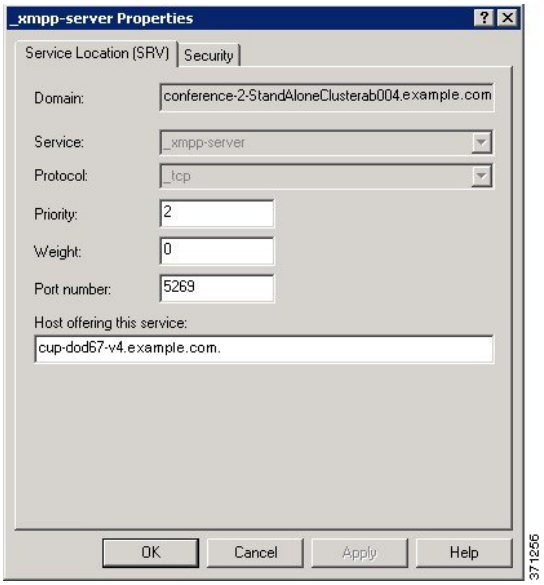


図 *6 :* チャット機能の *_xmpp-server* の *IPv6 DNS SRV* レコード

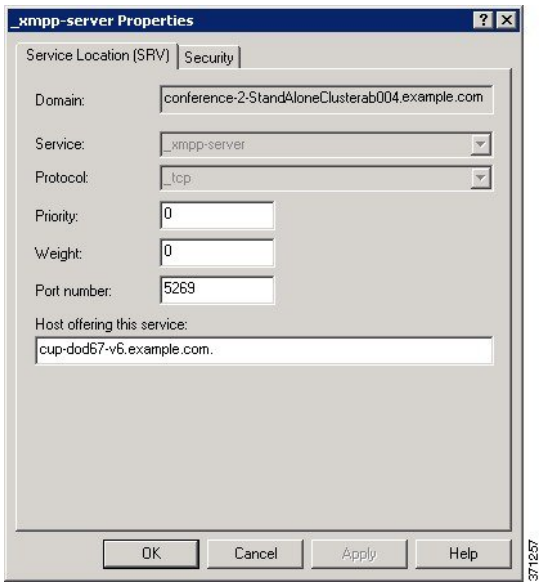
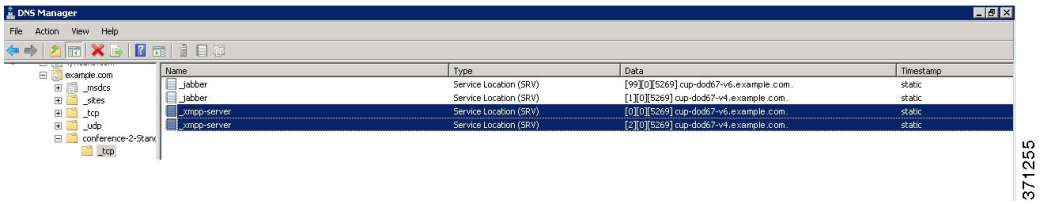


図 *7 :* チャット機能の *DNS* 構成



Configure MFT on XMPP Federation Without TLS

In this scenario, you must perform the following two extra steps for the MFT over XMPP Federation feature to work:

1. Extract file transfer aliases.
2. Create the DNS SRV records for file transfer aliases extracted in the previous step.

Before you begin

- Configure DNS SRV records for XMPP Federation. For more information, see XMPP フェデレーションの DNS SRV レコード, on page 6.
- Configure the Managed File Tranfer (MFT) feature as described in the Configuration and Administration of the IM and Presence Service guide for your release of Unified CM.

ステップ 1 To extract the file transfer aliases:

a) On each IM and Presence Service node where MFT is configured, create a CLI session and run **file build log cisco_xcp_config_mgr**.
b) Download the newly created archive and open `cm-5.xml` file.
c) The file transfer alias is stored with other MFT parameters in a common section of the file. In this example, you can find the file transfer alias in the following line:

```
<host-filter xmlns="http://www.jabber.com/config/cm/aft">
filetransfer-4-StandAloneClusterd41e3.cow.com
</host-filter>
```

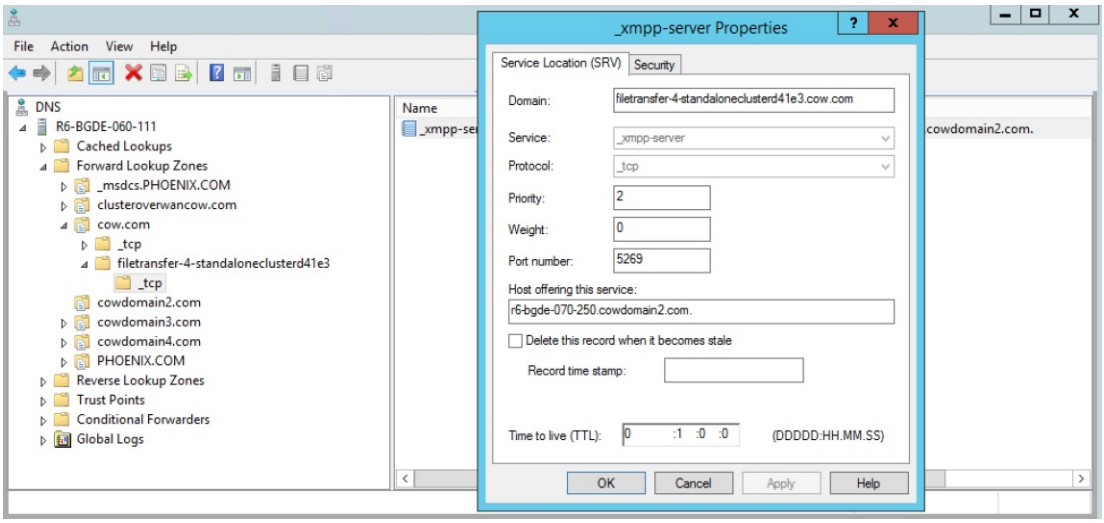
Important You must extract the file transfer aliases from each IM and Presence Service node which has MFT configured individually. Each node has its own unique alias that needs to be added to the DNS servers.

ステップ 2 Add aliases to the DNS server.

The file transfer alias extracted in the previous step belongs to the IM and Presence Service Publisher node (**r6-bgde-070-250.cowdomain2.com**) on the local side. We will use this alias as an example of how DNS records should be added.

The domains need to be added to DNS servers in the same way as the chat node aliases as described in XMPP フェデレーションのチャット ノードの DNS SRV レコードの構成, on page 10.

In the following screenshot, you can view the DNS SRV record for the file transfer alias.



Configure MFT on XMPP Federation with TLS

In this scenario, you must perform another step after extracting file transfer aliases and adding DNS SRV records as described in Configure MFT on XMPP Federation Without TLS, on page 12.

Perform the following steps on the local side:

Before you begin

Note

- We recommend that you use this method to configure MFT on XMPP Federation.
- To manually add file transfer aliases to the certificate, you must generate a CSR for the Multi SAN certificate. This is not possible in single node deployments. This is a limitation of this method.
- Use the following settings on the XMPP federation page on both sides:
  - **Security mode** must be set to TLS required.
  - The **Require client-side security certificates** checkbox must be checked.

For MFT on XMPP TLS federation to work, the cup -xmpp-s2s certificate must contain file transfer aliases. On IM and Presence Service, these file transfer aliases are not added automatically to the Certificate Signing Request (CSR). This default behavior can be overcome on a multinode IM and Presence Service cluster by generating and signing a Multi SAN certificate. However, on a single node cluster, it is impossible to generate a Multi SAN certificate CSR.

- Configure DNS SRV records for XMPP Federation. For more information, see XMPP フェデレーションの DNS SRV レコード, on page 6.
- Configure the Managed File Transfer (MFT) feature as described in the Configuration and Administration of the IM and Presence Service guide for your release of Unified CM.

ステップ 1 After extracting the file transfer aliases from all the nodes of the local cluster, generate a CSR for the MultiSan certificate.

ステップ 2 Log in to the **Cisco Unified IM and Presence OS Administration** page and choose **Security** > **Certificate Management**.

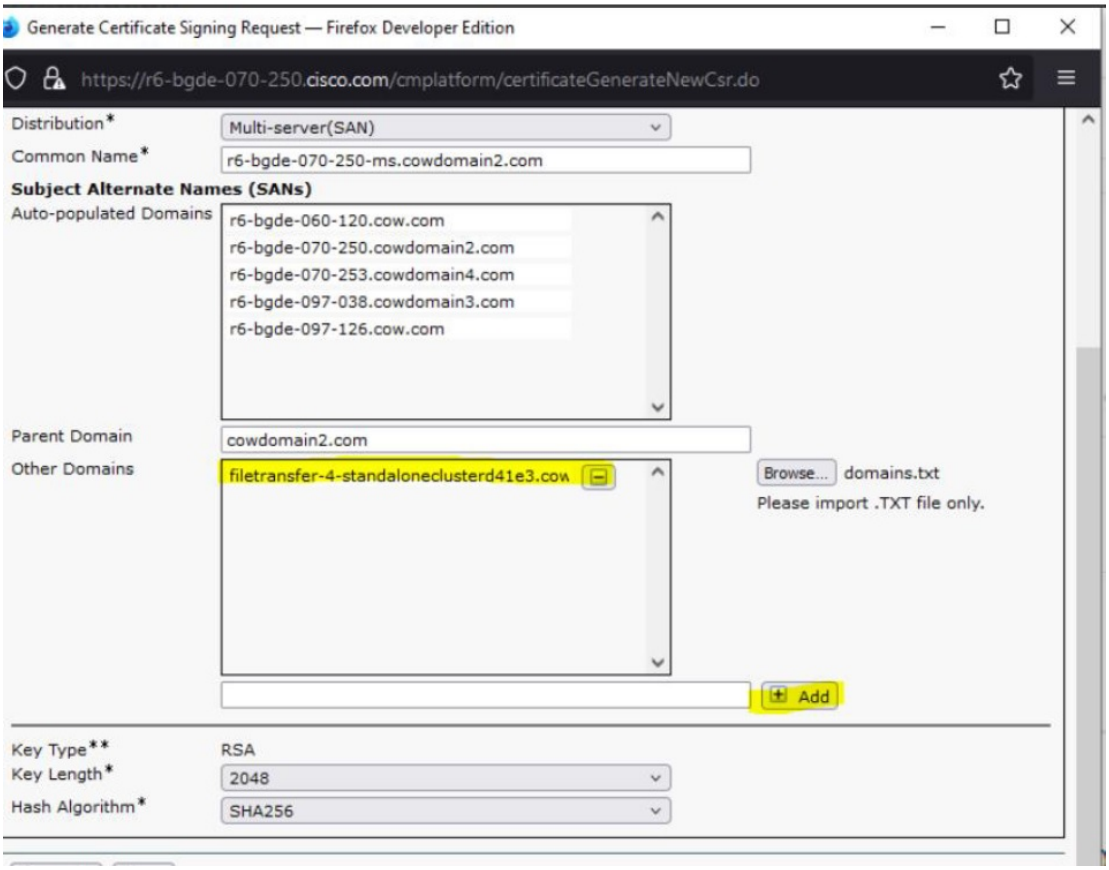
The **Certificate List** window appears.

ステップ 3 Click **Generate CSR**.

ステップ 4 From the **Certificate Purpose** drop-down list, choose **cup-xmpp-s2s**.

ステップ 5 From the **Distribution** drop-down list, choose **Multi-server(SAN)**.

ステップ 6 In the **Other Domains** section, add all file transfer aliases from the local cluster as shown in the following screenshot.



ステップ 7 Sign the cup-xmpp-s2s certificate using Certificate Authority.

ステップ 8 Upload the Root certificate and the newly signed Multi-SAN certificate according to the steps described in Upload a CA-Signed Certificate for XMPP Federation.

ステップ 9 Upload the Root certificate in the cup-xmpp-trust on the federated side.

Note Repeat all the above steps on the federated side.

XMPP フェデレーションのポリシー構成の構成

このセクションでは、XMPP フェデレーションのさまざまなポリシー設定構成について説明します。

ポリシー例外の構成

XMPP フェデレーションのデフォルトポリシーに対する例外を構成できます。例外では、例外を適用する外部ドメインと、例外の方向ルールを指定する必要があります。ポリシー例外のドメイン名を構成する場合は、次の点に注意してください。

- ユーザーの URI または JID が `user@example.com`の場合は、例外の外部ドメイン名を `example.com`として構成します。
- 外部企業がユーザーの URI または JID で hostname.domain を使用する場合（`user@hostname.example.com` など）、例外で外部ドメイン名を `hostname.example.com`として構成します。
- 例外の外部ドメイン名にワイルドカード（*）を使用できます。たとえば、値 `*.example.com`は、 `example.com`および example.com のサブドメイン（たとえば、どこか.example.com ）にポリシーを適用します。

また、 IM and Presence Service がポリシー例外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/ホストとの間で送受信されるすべてのフェデレーション パケット** ： IM and Presence Service は、指定されたドメインで送受信されるすべてのトラフィックを許可または拒否します。
- **上記のドメイン/ホストからの着信フェデレーション パケットのみ**：IM and Presence Service は指定されたドメインからのインバウンド ブロードキャストを受信できますが、 IM and Presence Service は応答を送信しません。
- **[上記のドメイン/ホストへの発信フェデレーション パケットのみ（Onlyouting federated packets to the above domain/host ）]**： IM and Presence Service が指定されたドメインにアウトバウンド ブロードキャストを送信することを許可しますが、 IM and Presence Service は応答を受信しません。

関連情報 -

XMPP フェデレーションのポリシーの構成

XMPP フェデレーションのポリシーの構成

注意 XMPP フェデレーション設定のいずれかに変更を加えた場合は、 **Cisco Unified IM and Presence Serviceability** のユーザー インターフェイスで、Cisco XCP ルータ（**[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）、Cisco XCP XMPP フェデレーション接続マネージャ（**[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]**）の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 によりすべての XCP サービスが再起動されます。

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（Interdomain 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 リストからポリシー設定を選択します。

- [許可（Allow）]： IM and Presence Service は、ポリシー例外リストで明示的に拒否したドメインを除き、XMPP フェデレーション ドメインからのすべてのフェデレーション トラフィックを許可します。
- [拒否（Deny）]： IM and Presence Service は、ポリシー例外リスト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ション トラフィックを拒否します。

ステップ 3 ポリシー例外リストにドメインを構成するには、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) ポリシー例外を適用する方向を指定します。
d) ポリシー例外ウィンドウで **[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。

関連情報 -

ポリシー例外の構成

XMPP フェデレーション用の Cisco 適応型セキュリティ アプライアンスの構成

XMPP フェデレーションの場合、Cisco 適応型セキュリティ アプライアンス はファイアウォールとしてのみ機能します。Cisco 適応型セキュリティ アプライアンスでは、XMPP フェデレーション トラフィックの着信と発信の両方に対してポート 5269 を開く必要があります。

これらは、Cisco 適応型セキュリティ アプライアンスリリース 8.3 でポート 5269 を開くアクセス リストの例です。

ポート 5269 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します。

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

任意のアドレスから任意の単一ノードへのポート 5269 でのトラフィックを許可します。

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

上記のアクセスリストを構成せず、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、これらの各ノードへのアクセスを設定する必要があります。次に例を示します。

```
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 コマンドを構成します。

手順

	コマンドまたはアクション	目的
ステップ 1	**nat (inside,outside) source static** *obj_host_private_imp1_ip obj_host_public_imp_ip* **service**	
ステップ 2	*obj_udp_source_eq_5269 obj_udp_source_eq_5269*	
ステップ 3	**nat (inside,outside) source static** *obj_host_private_imp1_ip obj_host_public_imp_ip* **service**	
ステップ 4	*obj_tcp_source_eq_5269 obj_tcp_source_eq_5269*	DNS で単一のパブリック IP アドレスを公開し、任意のポートを使用する場合は、次のように構成します。 （この例は、2 つの追加の XMPP フェデレーション ノード用です）
ステップ 5	**nat (inside,outside) source static** *obj_host_private_imp2_ip obj_host_public_imp_ip* **service**	
ステップ 6	*obj_udp_source_eq_5269 obj_udp_source_eq_25269*	
ステップ 7	**nat (inside,outside) source static** *obj_host_private_imp2_ip obj_host_public_imp_ip* **service**	
ステップ 8	*obj_tcp_source_eq_5269 obj_tcp_source_eq_25269*	
ステップ 9	**nat (inside,outside) source static** *obj_host_private_imp3_ip obj_host_public_imp_ip* **service**	
ステップ 10	*obj_udp_source_eq_5269 obj_udp_source_eq_35269*	
ステップ 11	**nat (inside,outside) source static** *obj_host_private_imp3_ip obj_host_public_imp_ip* **service**	
ステップ 12	*obj_tcp_source_eq_5269 obj_tcp_source_eq_35269*	DNS で複数のパブリック IP アドレスをすべてポート 5269 を使用して公開する場合は、次のように構成します。 （この例は、2 つの追加の XMPP フェデレーション ノード用です）

	コマンドまたはアクション	目的
ステップ 13	**nat (inside,outside) source static** *obj_host_private_imp2_ip obj_host_public_imp2_ip* **service**	
ステップ 14	*obj_udp_source_eq_5269 obj_udp_source_eq_5269*	
ステップ 15	**nat (inside,outside) source static** *obj_host_private_imp2_ip obj_host_public_imp2_ip* **service**	
ステップ 16	*obj_tcp_source_eq_5269 obj_tcp_source_eq_5269*	
ステップ 17	**nat (inside,outside) source static** *obj_host_private_imp3_ip obj_host_public_imp3_ip* **service**	
ステップ 18	*obj_udp_source_eq_5269 obj_udp_source_eq_5269*	
ステップ 19	**nat (inside,outside) source static** *obj_host_private_imp3_ip obj_host_public_imp_ip* **service**	
ステップ 20	*obj_tcp_source_eq_5269 obj_tcp_source_eq_5269*	**関連情報 -** SIP フェデレーションのための Cisco 適応型セキュリティアプライアンスの構成

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 Service ノードで Cisco XCP XMPP Federation Connection Manager サービスをオンにする必要があります。**[サービスのアクティブ化（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 Service が自動的にサービスを開始します。 **[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開始する必要はありません。

始める前に

Cisco 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。 「ノードでの XMPP フェデレーションの有効化 （4 ページ）」を参照してください。

ステップ 1 **Cisco Unified IM and Presence Serviceability** のユーザー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 [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 Service] 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。

関連情報 -

フェデレーションの有用性の設定

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。