XMPP フェデレーションに関する IM and Presence の設定

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 Release 9.0 は次のエンタープライズ バージョンの XMPP フェデレーションをサポートしています。

- Cisco WebEx Connect Release 6.0
- IBM Sametime Release 8.2 および 8.5
- GoogleTalk
- （別の）IM and Presence Release 9.0 Enterprise

（注） IM and Presence Service は IM and Presence Release 9.0 Enterprise から Cisco Unified Presence Release 7.x Enterprise の XMPP フェデレーションをサポートしていません。

IM and Presence 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 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 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 で XMPP フェデレーションをイネーブルにし、設定する必要があります。

複数の IM and Presence 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イネーブルにし、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 を配置する場合、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、および認証局（CA）の考慮事項については、統合の準備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、統合に関する Cisco Adaptive Security Appliance（ASA）の設定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

（注） XMPP フェデレーション設定のいずれかを変更する場合、IM and Presence Serviceability の Cisco XCP ルータ（[ツール（Tools）]>[コントロール センタのネットワーク サービス（Control Center - Network Services）] を選択します）、Cisco XCP XMPP Federation Connection Manager（[ツール（Tools）] > [コントロール センタの機能サービス（Control Center - Feature Services）]）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 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 の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [ドメイン間フェデレーション（Inter Domain Federation）CIMC] > [XMPP フェデレーション（XMPP Federation）] > [設定（Settings）] を選択します。
[XMPP フェデレーションのステータス（XMPP Federation Status）] メニューの [オン（On）] を選択します。

ステップ 2 [保存（Save）] を選択します。
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 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，（3 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 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 をイネーブルにする必要があります。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [ドメイン間フェデレーション（Inter Domain Federation）CIMC] > [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 メニューからセキュリティ モードを選択します。

a) [TLS なし（No TLS）] - IM and Presence 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 で、外部ドメインとの TLS 接続が試行されます。 IM and Presence 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 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）] 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）] をオンにしないでください。

ステップ 4 IM and Presence で着信接続の試行のために SASL EXTERNAL のサポートをアドバタイズするには、[すべての着信接続で SASL EXTERNAL を有効化（Enable SASL EXTERNAL on all incoming connections）] をオンにし、SASL EXTERNAL の検証を実装します。

ステップ 5 外部サーバから SASL EXTERNAL に要求する場合に IM and Presence から外部ドメインに必ず SASL 認証 ID を送信するには、[すべての発信接続で SASL EXTERNAL を有効化（Enabling SASL on outbound connections）] をオンにします。

ステップ 6 IM and Presence 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。 DNS によって外部サーバの ID が検証されるまで、IM and Presence で外部サーバのパケットは受け入れられません。

ステップ 7 [保存（Save）] を選択します。

トラブルシューティングのヒント

- 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展開の一部の場合、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, （2 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

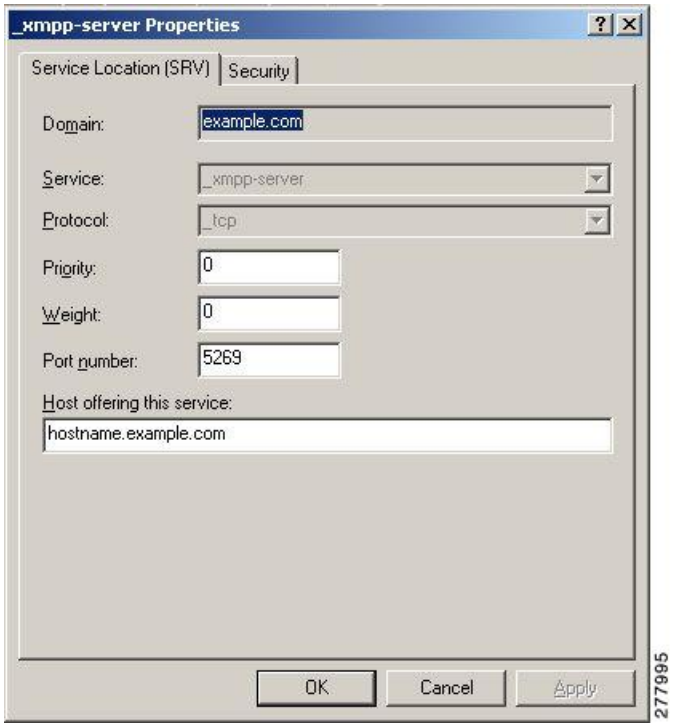
IM and Presence で特定の XMPP フェデレーテッド ドメインを検出できるようにするには、フェデレーテッド エンタープライズからパブリック DNS サーバの DNS SRV レコードを公開する必要があります。 同様に、IM and Presence でドメイン用に DNS と同じ DNS SRV レコードを公開する必要があります。 両方のエンタープライズはポート 5269 を公開する必要があります。 公開された FQDN は、DNS で IP アドレスに解決できる必要があります。

次のレコードが必要です。

"_xmpp-server._tcp.<domain>"

DNS SRV レコード "_xmpp-server" の DNS 設定例については、次の図を参照してください。

図 *1*：*"_xmpp-server"* の *DNS SRV*



IM and Presence 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。

```
nslookupset 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 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 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 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 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 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 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。

IM and Presence のクラスタ間配置およびマルチノード クラスタ配置では、外部の XMPP フェデレーテッド ドメインで新しいセッションが開始されると、その要求のルーティング先を決定するため DNS SRV ルックアップが実行されます。 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 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 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 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 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 で着信要求がロード バランシングされ、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が送信されます。

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, （6 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 サーバ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。

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。

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 PAT 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 でチャット機能を設定する方法については、IM and Presence Release 9.x の『Deployment Guide』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 レコードを設定する，（7 ページ）

XMPP フェデレーションのチャット ノード用 DNS SRV レコードを設定する

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 の管理（Cisco Unified CM IM and Presence Administration）] > [メッセージング（Messaging）] > [会議サーバ エイリアス マッピング（Conference Server Alias Mapping）] を選択します。

b) [検索（Find）] 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 ドメイン "StandAloneCluster" で、ドメイン "conference-2" を作成します。

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

ステップ 5 ドメイン "_tcp" で、"_xmpp-server" の新しい DNS SRV レコードを作成します。 DNS 設定例については、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 3 のドメインは "conference-2-StandAloneCluster" であり、手順 4 をスキップします。

図 *2*：チャット機能用の *"_xmpp-server"* の *DNS SRV*

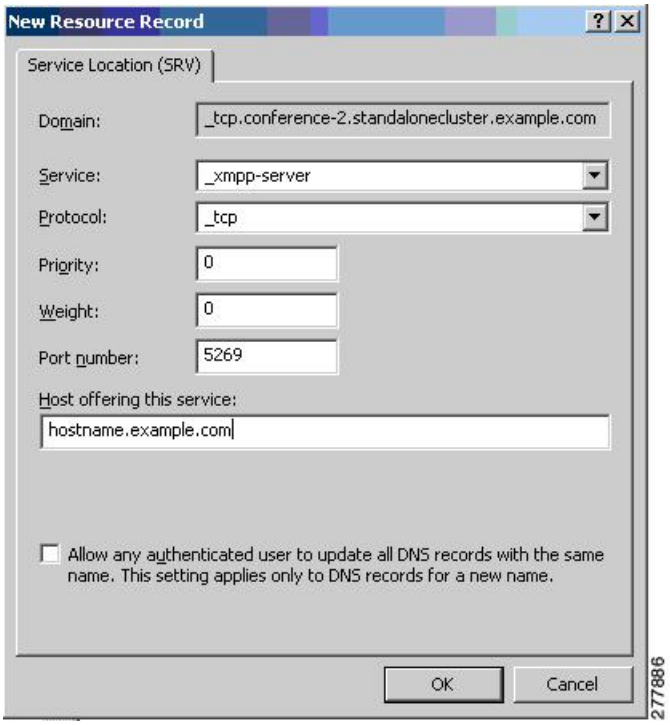


図 *3*：チャット機能用の *DNS* 設定

関連トピック

XMPP フェデレーション用 DNS SRV レコード, （4 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 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 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 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 から応答は送信しません。
- [上記のドメイン/ホストに発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 は指定したドメインに発信ブロードキャストを送信できますが、IM and Presence は応答を受信しません。

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, （10 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 の Cisco XCP ルータ（[ツール（Tools）] > [コントロール センタのネットワーク サービス（Control Center - Network Services）] を選択します）、Cisco XCP XMPP Federation Connection Manager（[ツール（Tools）] > [コントロール センタの機能サービス（Control Center - Feature Services）]）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 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 の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [ドメイン間フェデレーション（Inter Domain Federation）CIMC] > [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 メニューから次のポリシー設定を選択します。

- [許可（Allow）] - IM and Presence 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（Deby）] - IM and Presence 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：

a) [新規追加（Add New）] を選択します。
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）] を選択します。

ステップ 4 ポリシー ウィンドウで [保存（Save）] を選択します。
トラブルシューティングのヒント

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, （9 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 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 IM and Presence 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 cup ip address>#host <private cup ip
address>
object network obj_host_<private cup2 ip address>
#host <private cup2 ip address>
object network obj_host_<public cup ip address>
#host <public cup ip address>
```

....

次の NAT コマンドを設定します。

```
nat (inside,outside) source static obj_host_<private cup1 IP>
obj_host_<public cup IP> serviceobj_udp_source_eq_5269
obj_udp_source_eq_5269
nat (inside,outside) source static obj_host_<private cup1 IP>
obj_host_<public cup 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 cup2 ip>
obj_host_<public cup IP> serviceobj_udp_source_eq_5269
obj_udp_source_eq_25269
nat (inside,outside) source static obj_host_<private cup2 ip>
obj_host_<public cup IP> service
obj_tcp_source_eq_5269 obj_tcp_source_eq_25269

nat (inside,outside) source static obj_host_<private cup3 ip>
obj_host_<public cup IP> service
obj_udp_source_eq_5269 obj_udp_source_eq_35269
```

```
nat (inside,outside) source static obj_host_<private cup3 ip>
obj_host_<public cup 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 cup2 ip>
obj_host_<public cup2 IP> serviceobj_udp_source_eq_5269
obj_udp_source_eq_5269
nat (inside,outside) source static obj_host_<private cup2 ip>
obj_host_<public cup2 IP> service
obj_tcp_source_eq_5269 obj_tcp_source_eq_5269

nat (inside,outside) source static obj_host_<private cup3 ip>
obj_host_<public cup3 IP> service
obj_udp_source_eq_5269 obj_udp_source_eq_5269
nat (inside,outside) source static obj_host_<private cup3 ip>
obj_host_<public cup 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 フェデレーション用の電子メールをオンにする

IM and Presence で XMPP フェデレーション用の電子メールの使用をオンにすると、IM and Presence ではフェデレーション対象の各連絡先の JID が連絡先の電子メール アドレスに変更されます。

XMPP フェデレーション用の電子メールをオンにするには、SIP フェデレーションと同じ手順に従って操作します。詳細については、後述の「関連項目」の手順を参照してください。

現在、（XMPP フェデレーション配置の）フェデレーション機能の電子メール アドレスでは、マルチクラスタ IM and Presence 配置での一時的なチャット ルームとパーシステント チャット ルームをサポートしていません。 ローカル ドメインに複数の IM and Presence クラスタがある配置シナリオでは、ローカルユーザの実際の JID をフェデレーション対象ユーザに送信できます。 チャット ルームに対する唯一の影響は、フェデレーション対象ユーザに表示される名前が、ローカル ユーザの電子メール アドレスではなくローカル ユーザのユーザ ID であることです。その他のチャット ルームの機能は通常どおりに機能します。 このような状況は、フェデレーション対象ユーザとの一時的なチャット ルームとパーシステント チャット ルームでのみ発生します。

関連トピック

フェデレーション用電子メールの有効化

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 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。[サービスの開始（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 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 センタの機能サービス（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

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，（2 ページ）を参照してください。

手順

ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [ツール（Tools）] > [サービスの開始（Service Activation）] を選択します。

ステップ 2 [サーバ（Server）] リスト ボックスで、サーバを選択します。

ステップ 3 [移動（Go）] を選択します。

ステップ 4 [IM and Presence サービス（IM and Presence Services）] セクションで、[Cisco XCP XMPP Federation Connection Manager] サービスの横にあるオプション ボタンを選択します。

ステップ 5 [保存（Save）] を選択します。

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