



クラスタ間ピアの設定

- [クラスタ間ピアの概要](#) (1 ページ)
- [クラスタ間ピアの前提条件](#) (1 ページ)
- [クラスタ間ピアの設定のタスクフロー](#) (2 ページ)
- [クラスタ間ピアリングの連携動作と制限事項](#) (12 ページ)

クラスタ間ピアの概要

クラスタ間ピアにより、1つのクラスタ内のユーザが、同じドメイン内の異なるクラスタにいるユーザと通信したり、プレゼンスをサブスクライブしたりできます。大規模展開では、クラスタ間ピアリングを使用してリモート IM and Presence クラスタに接続できます。

クラスタ間ピアリングは、ローカルクラスタとリモートクラスタの両方のデータベースパブリッシュャノードで設定されます。

クラスタ間配置のサイズ設定とパフォーマンスの推奨事項については、http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/UCgoList.html#48016でCisco コラボレーションシステムソリューションリファレンスネットワークデザイン (SRND) の「コラボレーションインスタントメッセージおよびプレゼンス」を参照してください。

クラスタ間ピアの前提条件

ネットワークで IM and Presence Service クラスタ間ピアを設定する前に、次の点に注意してください。

- 必要に応じて全クラスタのシステム トポロジを設定し、ユーザを割り当てます。
- クラスタ間ピア接続が正常に機能するには、2つのクラスタ間にファイアウォールがある場合、次のポートが開いたままになっている必要があります。
 - 8443 (AXL)
 - 7400 (XMPP)
 - 5060 (SIP) (SIP フェデレーション使用時のみ)

- クラスタ間環境では、最小限の OVA を 15,000 ユーザに導入することを推奨します。すべてのクラスタが少なくとも 15,000 ユーザが OVA を実行している限り、複数のクラスタを異なる OVA のサイズで実行することが可能です。



(注) クラスタ間ピアリングは、Cisco Business Edition 6000 サーバに IM and Presence サービスが導入されている場合はサポートされません。

クラスタ間ピアの設定のタスクフロー

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザプロビジョニングを確認する (3 ページ)	クラスタ間ピアを設定する前に、エンドユーザが正しくプロビジョニングされていることを確認してください。
ステップ 2	Cisco AXL Web サービスの有効化 (3 ページ)	Cisco AXL Web サービスは、すべてのローカルおよびリモートの IM and Presence ノードでアクティブになっている必要があります。この手順を使用して、サービスが実行されていることを確認してください。
ステップ 3	同期エージェントを有効にする (4 ページ)	各クラスタ間ピアのデータベースパブリッシャノードで同期エージェントを有効にします。
ステップ 4	クラスタ間ピアの設定 (5 ページ)	クラスタ間ピアを設定するには、各クラスタのデータベースパブリッシャノードでこの作業を実行します。
ステップ 5	Intercluster Sync Agent がオンであることを確認します。 (7 ページ)	Intercluster Sync Agent は、IM and Presence Service クラスタ内のすべてのノードで実行されている必要があります。Intercluster Sync Agent パラメータが実行されていることを確認するには、この手順を使用します。
ステップ 6	クラスタ間ピア ステータスの確認 (8 ページ)	クラスタ間ピア設定が機能することを確認します。

	コマンドまたはアクション	目的
ステップ 7	Intercluster Sync Agent の Tomcat 信頼証明書の更新 (9 ページ)	クラスタ間ピアの tomcat 証明書のステータスが同期されない場合は、Tomcat 信頼証明書を更新する必要があります。
ステップ 8	クラスタ間ピアの定期同期エラーからの自動リカバリを有効化 (9 ページ)	クラスタ間ピアの定期同期エラーからの自動リカバリを有効にするには、次の手順を使用します。
ステップ 9	クラスタ間ピアの同期間隔の設定 (10 ページ)	クラスタ間ピアの同期の時間間隔を設定するには、次の手順を使用します。
ステップ 10	クライアント間ピア定期同期の証明書同期の無効化 (11 ページ)	証明書同期の無効化/有効化を、ホスト間定期同期の一部として設定するには、次の手順を使用します。

ユーザプロビジョニングを確認する

この手順を使用して、クラスタ間ピアを設定する前にエンドユーザが正しくプロビジョニングされていることを確認します。

手順

-
- ステップ 1 Cisco Unified CM IM and Presence Administration から、**[診断 (Diagnostics)]** > **[システムトラブルシューター (System Troubleshooter)]** を選択します。
システムトラブルシューターが実行されます。
 - ステップ 2 ユーザトラブルシューターセクションで、エンドユーザが正しくプロビジョニングされていること、および重複または無効なユーザがないことを確認します。
-

次のタスク

[Cisco AXL Web サービスの有効化 \(3 ページ\)](#)

Cisco AXL Web サービスの有効化

Cisco AXL Web サービスは、すべてのローカルとリモートの IM and Presence クラスタノードで実行されている必要があります。デフォルトにより、このサービスは実行されます。ただし、この手順を使用してサービスが実行されていることを確認できます。



- (注) Cisco AXL Web サービスを有効にすると、システムは AXL 権限を持つクラスタ間アプリケーションユーザを作成します。リモートの IM and Presence Service ノードでクラスタ間ピアを設定するには、クラスタ間アプリケーションユーザのユーザ名とパスワードが必要です。

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)] から、[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。
- ステップ 2** [サーバ (Server)] リストから、サービスを再アクティブ化するノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3** [データベースおよび管理サービス (Database and Admin Services)] エリアで、[Cisco AXL Web サービス (Cisco AXL Web Service)] の[状態]を選択します。
- サービスが起動したら、アクションは不要です。
 - サービスが実行されていない場合は、サービスを選択して[再起動 (Restart)] をクリックします。
- ステップ 4** ローカルクラスタとリモートクラスタのすべてのクラスタノードでこの手順を繰り返します。

次のタスク

[同期エージェントを有効にする \(4 ページ\)](#)

同期エージェントを有効にする

Cisco Sync Agent は、ローカルおよびリモートの各クラスタ間ピアのデータベースパブリッシャノードで実行している必要があります IM and Presence データベースパブリッシャノード。

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)] から、[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。
- ステップ 2** [サーバ (Server)] ドロップダウンリスト ボックスから、IM and Presence データベースパブリッシャノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3** IM and Presence サービスで、Cisco Sync Agent ステータスが実行中であることを確認します。
- ステップ 4** サービスが実行されていない場合は、サービスを選択して[再起動 (Restart)] をクリックします。

ステップ5 クラスタ内ごとに、この手順を繰り返します。

次のタスク

Cisco Sync Agent が Cisco Unified Communications Manager からのユーザ同期を完了した後、[クラスタ間ピアの設定 \(5 ページ\)](#)

クラスタ間ピアの設定

ローカルクラスタとリモートクラスタの両方のデータベースパブリッシャノードでこの手順を使用して、クラスタ間ピア関係を設定します。

始める前に

- Sync Agent がローカルクラスタとリモートクラスタのCisco Unified Communications Manager からのユーザ同期化を完了したことを確認します。Sync Agent がユーザの同期化を完了する前にクラスタ間ピア接続を設定した場合は、クラスタ間ピア接続のステータスは**失敗**として表示されます。
- リモートの IM and Presence サービス ノードのクラスタ間アプリケーションユーザの AXL ユーザ名とパスワードを取得していることを確認します。

手順

ステップ1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[**プレゼンス (Presence)**]>[**クラスタ間 (Inter-Clustering)**] を選択します。

ステップ2 [新規追加 (Add New)] をクリックします。

ステップ3 [**ピアアドレス (Peer address)**] フィールドに、リモートクラスタのデータベースパブリッシャノードのノード名を入力します。このフィールドは IP アドレス、ホスト名、または FQDN ですが、サーバを定義する実際のノード名と一致している必要があります。

(注) ・ノード名が使用するアドレスのタイプを確認するには、リモートクラスタ上の Cisco Unified CM IM and Presence 管理にログインして、**システム > プレゼンス トポロジ**を選択します。このウィンドウには、各クラスタノードのノード名およびサーバの詳細が表示されます。

・マルチクラスタ環境の一部のクラスタでは、スプリットブレイン現象が発生する場合があります。たとえば、クラスタ A があった場合、マルチクラスタのピアはクラスタ B、C、D、および E があるとします。クラスタ A 内のノードは、スプリットブレイン現象の際に、マルチクラスタ環境の他のクラスタ B、C、D、E と通信する必要があるため、スプリットブレイン現象の発生中に DNS にアクセス可能である必要があります。

スプリットブレイン現象が発生して、クラスタ A のノードが DNS にアクセスできない場合、A、B、C、D、および E クラスタノードの IP アドレスは、ホスト名と FQDN ではなく、ノード名として設定する必要があります。

クラスタ A、B、C、および E のノードが FQDN またはホスト名を使用して定義されていると、スプリットブレイン現象が発生して DNS にアクセスできない場合、IM Presence 情報が失われたり、クラスタ A と B、C、D、E 間での IM 履歴が失われたりするなど、サービス障害が発生します。

ステップ 4 AXL クレデンシャルの入力

ステップ 5 SIP 通信の優先プロトコルを入力します。

(注) すべての IM and Presence サービスクラスタのクラスタ間トランク転送として **TCP** (デフォルト設定) を使用することを推奨します。この設定がネットワーク構成とセキュリティのニーズに合っている場合は、この設定を変更できます。

ステップ 6 [保存 (Save)]をクリックします。

ステップ 7 GUI ヘッダーの右上にある通知を確認します。Cisco XCP ルータを再起動するように通知された場合、次の操作を行います。それ以外の場合は、このステップを省略できます。

- a) [Cisco Unified IM and Presence のサービスアビリティ (Cisco Unified IM and Presence Serviceability)] から、[ツール (Tools)] > [コントロールセンタ-ネットワークサービス (Control Center - Network Services)] を選択します。
- b) [サーバ (Server)] ドロップリストボックスから、IM and Presence ノードを選択して、[移動 (Go)] をクリックします。
- c) [Cisco XCP Router] を選択し、[リスタート (Restart)] をクリックします。
- d) 全クラスタ ノードで上記の手順を繰り返します。

ステップ 8 各リモートピアクラスタのデータベースパブリッシャノードでこの手順を繰り返します。

ヒント クラスタ間転送プロトコルとして **TLS** を選択する場合は、**IM and Presence** サービスは、クラスタ間ピアの間で証明書を自動的に交換して、セキュアな TLS 接続を確立しようとしています。**IM and Presence** サービスは、証明書交換がクラスタ間ピアのステータスのセクションで正常に行われるかどうかを示します。

次のタスク

[Intercluster Sync Agent がオンであることを確認します。](#) (7 ページ)

XCP ルータ サービスを再起動します。

ローカルクラスタ内のすべてのノードで Cisco XCP Router サービスを再起動します。リモートクラスタの全ノードでも同様にします。

始める前に

[クラスタ間ピアの設定](#) (5 ページ)

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)] から、[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。
 - ステップ 2** [サーバ (Server)] リストから、サービスを再アクティブ化するノードを選択し、[移動 (Go)] をクリックします。
 - ステップ 3** [IM and Presence サービス (IM and Presence Services)] 領域で、[Cisco XCP Router] を選択します。
 - ステップ 4** [再起動 (Restart)] をクリックします。
-

次のタスク

[Intercluster Sync Agent がオンであることを確認します。](#) (7 ページ)

Intercluster Sync Agent がオンであることを確認します。

クラスタ間同期エージェントネットワークサービスは、クラスタ間ピア間でユーザ情報を同期します。この手順を使用して、各クラスタ間ピアのすべてのクラスタノードでサービスが実行されていることを確認します。

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)] から、[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。
- ステップ 2 [サーバ (Server)] メニューから、IM and Presence サービス ノードを選択し、[移動 (Go)] をクリックします。
- ステップ 3 Cisco クラスタ間同期エージェントが実行ステータスを表示していることを確認します。
- ステップ 4 サービスが実行されていない場合は、サービスを選択して[起動 (Start)] をクリックします。
- ステップ 5 各クラスタ間ピアの全クラスタ ノードに対してこの手順を繰り返します。

次のタスク

[クラスタ間ピア ステータスの確認 \(8 ページ\)](#)

クラスタ間ピア ステータスの確認

この手順を使用して、クラスタ間ピア設定が正しく機能していることを確認します。

手順

- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[プレゼンス (Presence)]>[クラスタ間 (Inter-Clustering)] を選択します。
- ステップ 2 検索条件メニューからピア アドレスを選択します。
- ステップ 3 [検索 (Find)] をクリックします。
- ステップ 4 [クラスタ間ピア ステータス (Inter-cluster Peer Status)] ウィンドウで次の操作を実行します。
 - a) クラスタ間ピアの各結果エントリの横にチェック マークがあることを確認します。
 - b) [関連ユーザ (Associated Users)] の値がリモートクラスタのユーザ数と等しいことを確認します。
 - c) クラスタ間転送プロトコルとして TLS を選択した場合は、[証明書のステータス (Certificate Status)] 項目に TLS 接続のステータスが表示され、IM and Presence Service が正常にクラスタ間でセキュリティ証明書を交換したかが示されます。証明書が同期されない場合は、(このモジュールで説明されているように) 手動で Tomcat 信頼証明書を更新する必要があります。その他の証明書交換エラーについては、オンラインヘルプで推奨処置を確認してください。
- ステップ 5 システムトラブルシューターを実行します。
 - a) Cisco Unified CM IM and Presence Administration から、[診断 (Diagnostics)]>[システムトラブルシューター (System Troubleshooter)] を選択します。

- b) [クラスタ間トラブルシュータ (Inter-Clustering Troubleshooter)] セクションで、各クラスタ間ピア接続エントリのステータスの横にチェック マークがあることを確認します。

次のタスク

[Intercluster Sync Agent の Tomcat 信頼証明書の更新 \(9 ページ\)](#)

Intercluster Sync Agent の Tomcat 信頼証明書の更新

接続エラーがローカル クラスタで発生した場合、および「破損した」Tomcat 信頼証明書がリモート クラスタに関連付けられている場合、この手順を使用して Tomcat 信頼証明書を更新します。

クラスタ間ピアの tomcat 証明書のステータスが同期されない場合は、Tomcat 信頼証明書を更新する必要があります。クラスタ間展開では、新しいリモート クラスタを指すように既存のクラスタ間ピア設定を再利用する場合にこのエラーが発生します。このエラーは、初めて IM and Presence をインストールしたとき、または IM and Presence Service のホスト名またはドメイン名を変更した場合、あるいは Tomcat 証明書を再生成した場合にも発生することがあります。

手順

-
- ステップ 1** [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[プレゼンス (Presence)] > [クラスタ間 (Inter-Clustering)] を選択します。
- ステップ 2** リモート クラスタと証明書を同期するには、[強制同期 (Force Sync)] を選択します。
- ステップ 3** 表示される確認ウィンドウで、[ピアの Tomcat 証明書も再同期 (Also resync peer's Tomcat certificates)] を選択します。
- ステップ 4** [OK] をクリックします。

(注) 自動的に同期していない証明書がある場合は、[Intercluster Peer Configuration] ウィンドウに進みます。X でマークされた証明書はすべて、不足している証明書であり、手動でコピーする必要があります。

クラスタ間ピアの定期同期エラーからの自動リカバリを有効化

Cisco Intercluster Sync Agent が「InterClusterSyncAgentPeerPeriodicSyncingFailure」アラームを発生させ、Intercluster ピアの定期的な同期が 2 時間を超えた場合に自動的に再起動するようにするには、この手順を使用してこのサービスパラメータを有効にします。

手順

-
- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[システム (System)] > [サービス パラメータ (Service Parameters)] を選択します。
- ステップ 2 [サーバ (Server)] リストから、「Intercluster Sync Agent の一般的なパラメータ」を設定する IM and Presence ノードを選択します。
- ステップ 3 サービスリストから、**Cisco Intercluster Sync Agent(Active)**を選択します。
- ステップ 4 をセットするクラスタ間ピアの定期同期エラーに対する自動回復を有効にするサービスパラメータ有効にします。
- ステップ 5 [保存 (Save)] をクリックします。

(注) あれば「クラスタ間ピア定期同期エラーに対する自動回復を有効にする」 service パラメータが Enabled に設定されており、定期的な同期が 2 時間を超えて停止した場合

- **InterClusterSyncAgentPeerPeriodicSyncingFailure** アラームが発生します。
- **Cisco** クラスタ間同期エージェントサービスは自動的に再開されます。

「クラスタ間ピア定期同期エラーの自動回復を有効にする」が無効になっている場合は、

- **InterClusterSyncAgentPeerPeriodicSyncingFailure** アラームが発生します。
 - **Cisco** クラスタ間同期エージェント サービスは自動的に再開されません。
-

クラスタ間ピアの同期間隔の設定

クラスタ間ピアの同期の時間間隔を設定するには、次の手順を使用します。サービスパラメータ [クラスタ間ピアの定期同期間隔 (分) (Inter Cluster Peer Periodic Sync Interval (mins))] を使用すると、ダイナミック ICSA の定期同期の時間間隔を設定できます。クラスタ間ピアの同期間隔のデフォルト設定は 30 分です。

手順

-
- ステップ 1 [Cisco Unified CM IM and Presence の管理 (Cisco Unified CM IM and Presence Administration)] で、[システム (System)] > [サービス パラメータ (Service Parameters)] を選択します。
- ステップ 2 [サーバ (Server)] リストから、「Intercluster Sync Agent の一般的なパラメータ」を設定する IM and Presence ノードを選択します。
- ステップ 3 サービスリストから、**Cisco Intercluster Sync Agent(Active)**を選択します。
- ステップ 4 [クラスタ間ピアの定期同期間隔 (分) (Inter Cluster Peer Periodic Sync Interval (mins))] サービスパラメータを適切な間隔に設定します。指定範囲は 30 ~ 1444 分で、デフォルトは 30 分です。

ステップ5 [保存 (Save)] をクリックします。

(注) 新しい設定は、次のクラスタ間同期の実行時から有効になります。

クラスタ間ピアの同期に失敗すると、Cisco Intercluster Sync Agent サービスは同期間隔を4回完了した後に再起動します。たとえば、このパラメータが40分に設定されている場合、サービスは160分(4*40)後に再起動します。

クライアント間ピア定期同期の証明書同期の無効化

証明書同期を、証明書間同期プロセスの一部として無効にするには、次の手順を使用します。クラスタ間定期同期中のサービスパラメータ証明書同期では、管理者がクラスタ間定期同期の一部として証明書同期を無効または有効にできます。このサービスパラメータのデフォルト値は、証明書同期の実行 (Perform certificate sync) 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)] で、[システム (System)] > [サービス パラメータ (Service Parameters)] を選択します。

ステップ2 [サーバ (Server)] リストから、Intercluster Sync Agent の一般的なパラメータを設定する IM and Presence ノードを選択します。

ステップ3 サービスリストから、Cisco Intercluster Sync Agent(Active)を選択します。

ステップ4 クラスタ間定期同期中にサービスパラメータの証明書同期を [証明書同期を実行しない (Do not perform certificate sync)] に設定します。

ステップ5 [保存 (Save)] をクリックします。

(注) 展開環境で、証明書の同期に関連する、証明書の定期同期中にパフォーマンスの低下またはCPU使用率の増加が発生した場合は、次の手順を使用してサービスパラメータを設定できます。

クラスタ間ピア接続の削除

クラスタ間ピア関係を削除する場合は、この手順を使用します。

手順

ステップ1 IM and Presence サービスのデータベース パブリッシャ ノードにログインします。

ステップ2 Cisco Unified CM IM and Presence 管理で、プレゼンス(Presence) > クラスタ間(Inter-Clustering) を選択します。

ステップ3 [検索(Find)]をクリックし、削除するクラスタ間ピアを選択します。

ステップ4 [削除 (Delete)]をクリックします。

ステップ5 ピア クラスタでこれらの手順を繰り返します。

(注) IM and Presence サービスが拡張され、クラスタ間ピアを削除した後、IM and Presence クラスタ内の各ノードで XCP ルータが再起動されるのを防ぐためです。この機能拡張により、管理者はノードのシーケンシャル再起動によるオーバーヘッドを大幅に軽減し、Jabber サービスを停止することで、大規模クラスタを効果的に管理できます。

クラスタ間ピアリングの連携動作と制限事項

機能	連携動作と制限事項
Cisco Business Edition 6000	クラスタ間ピアリングは、Cisco Business Edition 6000 サーバに IM and Presence サービスが導入されている場合はサポートされません。
クラスタ制限 (Cluster Limit)	クラスタ間ピアリングを使用すると、クラスタ間メッシュに最大 30 個の IM and Presence サービス クラスタをデプロイできます。
マルチクラスタ展開でのクラスタ間同期エージェントのリソース不足	<p>ICSA では、多数のクラスタを持つマルチクラスタ展開では、より多くのリソースが必要になります。リソース不足のため、ICSA または SRM に関する問題に直面した場合に備えて次に示す Cisco SIP プロキシ サービス パラメータをデフォルト値の 20 から 10 の新しい値に変更することをお勧めします。</p> <ul style="list-style-type: none"> • 最大プロセス数 • 最大スベアプロセス数 • 最大プロセス数 <p>変更を有効にするには、SIP プロキシ サービスを再起動します。</p> <p>SRM および ICSA サービスを再起動します。</p>