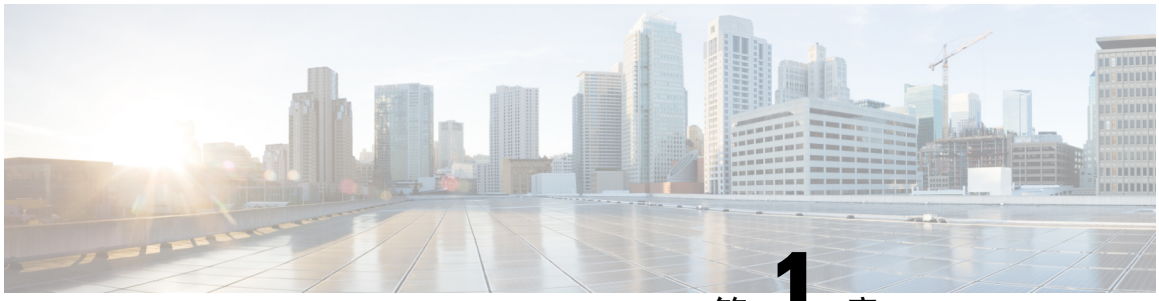
IM and Presence Service リリース 15 の設定と管理

First Published: 2023-12-18

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2023 Cisco Systems, Inc. All rights reserved.

CONTENTS



第 1 章

新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

次の表は、この最新リリースまでのガイドでの機能の主な変更点の概要を示したものです。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

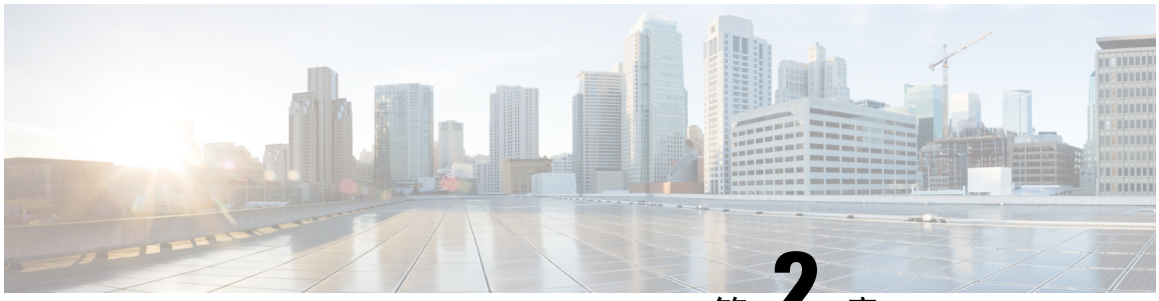
***Table 1: IM and Presence* サービスの新機能と変更された動作**

日付	説明	参照先
2023 年 12 月 18 日	Microsoft リモートコール制御機能の削除。	-

新機能および変更された機能に関する情報

第 I 部

システム計画



第 2 章

システム計画

IM and Presence Service の概要

IM and Presence サービスの管理は、IM and Presence サービスノードに対する個々の設定変更を、手動で行うための web ベースのアプリケーションです。このガイドの手順では、このアプリケーションを使用して機能を設定する方法について説明します。

IM and Presence サービスは、豊富な機能を備えた Cisco Jabber ユニファイドコミュニケーションクライアント、またはサードパーティの XMPP 対応 IM and Presence クライアントのいずれかを選択できます。IM and Presence サービスは、インスタントメッセージング、ファイル転送を提供し、さらに、固定グループチャットルームをホストしたり、設定したりすることができます。

Cisco Unified Communications Manager IM and Presence サービスによるオンプレミス展開で使用可能なサービスは次のとおりです。

- プレゼンス
- Instant Messaging（インスタント メッセージング）
- ファイル転送
- 音声通話（Audio Calls）
- ビデオ

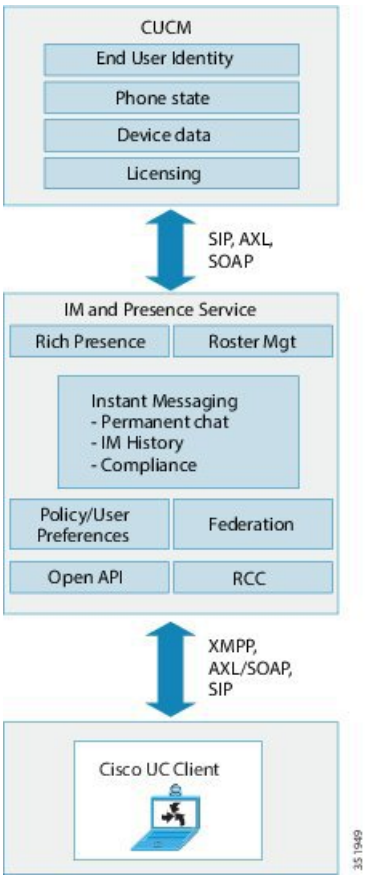
- ボイスメール
- 会議

詳細は、Cisco Unified Communications Manager のマニュアル を参照してください。

IM and Presence Service のコンポーネント

次の図は、主なコンポーネントや Cisco Unified Communications Manager と IM and Presence Service 間のインターフェイスなど、IM and Presence Service 展開の概要を示します。

図 *1 : IM and Presence Service* の基本的な展開



SIP インターフェイス

SIP インターフェイスを有効にするには、以下の設定を行う必要があります。

- Cisco Unified Communications Manager の SIP 接続を有効にするには、SIP トランクを IM and Presence サーバを指すように設定する必要があります。
- IM and Presence サービス で、Cisco Unified Communications Manager をプレゼンスゲートウェイとして設定すると、IM and Presence で SIP トランクを介して SIP SUBSCRIBE メッセージを Cisco Unified Communications Manager に送信することができます。

AXL/SOAP インターフェイス

AXL/SOAP インターフェイスは、Cisco Unified Communications Manager からのデータベースの同期を処理し、IM and Presence Service データベースにデータを入力します。データベース同期をアクティブにするには、Sync Agent サービスが IM and Presence で実行されている必要があります。

Sync Agent は、デフォルトでは M and Presence Service クラスタ内のすべてのノードにすべてのユーザを等しくロードバランシングします。ただし、クラスタ内の特定のノードにユーザを手動で割り当てることもできます。

シングルおよびデュアル ノードの IM and Presence Service で Cisco Unified Communications Manager とのデータベース同期を実行する場合の推奨される同期化間隔については、IM and Presence Service の SRND マニュアルを参照してください。

（注） AXL インターフェイスは、アプリケーション開発者の連係動作がサポートされていません。

LDAP インターフェイス

Cisco Unified Communications Manager は、すべてのユーザ情報を手動設定または LDAP を介した直接同期によって取得します。IM and Presence Service は、Cisco Unified Communications Manager からこのユーザ情報をすべて同期します（AXL/SOAP インターフェイスを使用）。

IM and Presence Service は、Cisco Jabber クライアントのユーザの LDAP 認証および IM and Presence Service ユーザ インターフェイスを提供します。Cisco Jabber ユーザが IM and Presence Service にログインし、LDAP 認証が Cisco Unified Communications Manager で有効になっている場合、IM and Presence Service はユーザ認証用の LDAP ディレクトリに直接移動します。ユーザが認証されると、IM and Presence Service は Cisco Jabber にこの情報を転送し、ユーザ ログインを続行します。

XMPP インターフェイス

XMPP 接続は、XMPP ベースのクライアントのプレゼンス情報交換やインスタント メッセージ動作を処理します。IM and Presence サービスは、XMPP ベースのクライアントの一時的（アドホック）および永続的（常設）チャットルームをサポートします。IM ゲートウェイは、IM and Presence サービス展開における SIP ベースのクライアントと XMPP ベースのクライアント間の IM 相互運用性をサポートします。

CTI インターフェイス

CTI（コンピュータ テレフォニー インテグレーション）インターフェイスは、IM and Presence ノードにおけるユーザのすべての CTI 通信を処理して、Cisco Unified Communications Manager 上の電話機を制御します。CTI 機能を使用すると、Cisco Jabber クライアントのユーザはデスクフォン制御モードでアプリケーションを実行できます。

Cisco Unified Communications Manager の IM and Presence Service ユーザの CTI 機能を設定するには、ユーザが CTI 対応グループに関連付けられ、そのユーザに割り当てられているプライマリ内線が CTI に対応している必要があります。

Cisco Jabber デスクフォン制御を設定するには、CTI サーバおよびプロファイルを設定し、そのプロファイルにデスクフォン モードでアプリケーションを使用するユーザを割り当てる必要があります。ただし、すべての CTI 通信は Cisco Unified Communications Manager と Cisco Jabber の間で直接実行され、IM and Presence Service サーバを介しません。

Cisco IM and Presence Data Monitor サービス

Cisco IM and Presence Data Monitor は、IM and Presence Service の IDS レプリケーションのステータスを監視します。その他の IM and Presence サービスは、Cisco IM and Presence Data Monitor に依存しており、IDS レプリケーションが安定した状態になるまで起動が遅延する場合があります。

Cisco IM and Presence Data Monitor は、Cisco Unified Communications Manager から Cisco Sync Agent の同期のステータスをチェックします。IDS レプリケーションをセットアップし、IM and Presence データベース パブリッシャ ノードで Sync Agent が Cisco Unified Communications Manager リリースからの同期を完了した後でのみ、依存するサービスの起動が許可されます。タイムアウトが発生すると、IDS レプリケーションおよび Sync Agent が完了していない場合でも、パブリッシャ ノードの Cisco IM and Presence Data Monitor により依存するサービスの起動が許可されます。

サブスクライバ ノードでは、IDS レプリケーションが正常に確立されるまで Cisco IM and Presence Data Monitor は機能サービスの起動を遅らせます。Cisco IM and Presence Data Monitor は、クラスタ内の問題のあるサブスクライバ ノードのみで機能サービスの起動を遅らせます。1 台のノードで問題があっても、すべてのサブスクライバ ノードで機能サービスの起動が遅れることはありません。たとえば IDS レプリケーションが node1 および node2 で正常に確立されていても、node3 で確立されていない場合、Cisco IM and Presence Data Monitor は機能サービスを node1 および node2 で起動しますが、node3 では起動を遅らせます。

Cisco IM and Presence Data Monitor は、IM and Presence データベース パブリッシャ ノードで異なる動作をします。Cisco UP Replication Watcher サービスは、タイムアウトが発生するまで機能サービスの開始を遅らせます。タイムアウトが発生すると、IDS の複製が正常に確立されていなくても、パブリッシャ ノード上ですべての機能サービスの開始を許可します。

ノードの機能サービスの起動を遅らせる場合は、Cisco IM and Presence Data Monitor がアラームを生成します。次に、IDS の複製がそのノードで正常に確立されたときに通知を生成します。

Cisco IM and Presence Data Monitor は、新しいマルチノード インストールと、ソフトウェア更新手順の両方に影響します。パブリッシャ ノードおよびサブスクライバ ノードが同じ IM and Presence リリースを実行し、IDS の複製がサブスクライバ ノードで正常に確立された場合にのみ両方が完了します。

ノードの IDS 複製のステータスを確認するには、次の手順を実行します。

- 使用する CLI コマンド：`utils dbreplication runtimestate`
- Cisco Unified IM and Presence Reporting Tool を使用します。IM and Presence Database Status レポートに、クラスタの詳細なステータスが表示されます。

Cisco Sync Agent のステータスを確認するには、Cisco Unified CM IM and Presence の管理インターフェイスに移動し、[診断]>[システムダッシュボード]を選択します。Cisco Unified Communications Manager の ノード IP アドレスと同期ステータスが確認できます。

計画の概要

システムを設定する前に、システム導入方法の計画を必ず立ててください。IM and Presence Service は、幅広い導入オプションを提供しており、企業のさまざまなニーズを満たす設計になっています。

個別のニーズを満たす IM and Presence Service の展開を含む Cisco Collaboration システムの設計方法の詳細は、http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.htmlの *Cisco Collaboration System Solution* 参照ネットワーク設計 を参照してください。

導入を計画する

システムを設定する前に、クラスタ トポロジおよびシステム導入方法を必ず計画してください。

手順

	コマンドまたはアクション	目的
Step 1	コラボレーション導入のサイジング	全体的なサイジングの推奨事項については、http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html の『Cisco Collaboration システム ソリューション リファレンス ネットワーク設計』の「Collaboration Solution サイジング ガイド」の章を参照してください。
Step 2	導入する機能を決定します。	詳細については、「機能の導入オプション（10 ページ）」を参照してください。
Step 3	標準的な導入または IM and Presence 中央クラスタを導入するかどうかを決定する	IM and Presence Service をテレフォニーと同じクラスタ展開するか、IM and Presence の集中型クラスタを展開するかを決めます。詳細については、標準導入 vs 中央クラスタを参照してください。
Step 4	導入するクラスタ ノード数の計画を立てます。	IM and Presence Service のマルチノードの拡張性機能を使用すると、必要に応じた展開のサイジングが可能です。詳細については、「マルチノードの拡張性要件（14 ページ）」を参照してください。
Step 5	冗長性を追加する方法を計画します。	展開の拡張性オプション（16 ページ）

	コマンドまたはアクション	目的
Step 6	地理的サイトの計画	ハードウェアを単一のロケーションからメンテナンスするために、単一のサイトにインストールすることができます。ただし、WAN を介してクラスタを展開し、複数のサイトを展開することで、地理的な冗長性を追加することも可能です。詳細については、次の項を参照してください。 • WAN 経由のクラスタ内展開（18 ページ） • WAN 経由のクラスタ間展開（19 ページ）
Step 7	IM and Presence ユーザーの Jabber 識別子（JID）のスキーマを計画します。	Jabber 識別子（JID）で使用できる文字については、RFC 3920（3. アドレス方式）および XEP-0106 を参照してください。Cisco Jabber およびその他のサードパーティ XMPP クライアントは、クライアント側のドキュメントを参照する必要がある追加の制限を課す場合があります。
Step 8	SAML シングル サインオンを設定するかどうかを決定します。	詳細については、「SAML シングル サインオンの展開（20 ページ）」を参照してください。
Step 9	サードパーティのアプリケーションと統合するかどうかを決定します。	これには、Microsoft Outlook カレンダーとの統合だけでなく、サードパーティ システムとの連携を含みます。詳細については、「サード パーティ統合（20 ページ）」を参照してください。

IM and Presence のサイジング展開

Collaboration 導入のサイジング方法の詳細は、http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html にある『*Cisco Collaboration* システム ソリューション リファレンス ネットワーク設計』の「Collaboration Solution サイジング ガイド」の章を参照してください。

機能の導入オプション

IM and Presence Service をインストールし、基本的な展開でユーザを設定した後に使用できる主な機能には、基本 IM、可用性、アドホック グループ チャットの機能があります。

オプション機能を追加することで、基本的な展開を拡張できます。次の図に、IM and Presence Service の機能展開オプションを示します。

次の表に、IM and Presence Service の機能展開オプションのリストを示します。

表 *2 : IM and Presence Service* 機能の展開オプション

コア IM とアベイラビリティ機能	高度な IM 機能（オプション）	豊富な Unified Communications アベイラビリティ機能（オプション）	リモート デスク フォン制御（オプション）
ユーザ アベイラビリティの表示 リッチテキスト IM のセキュアな送受信 ファイル転送 アドホック グループ チャット 連絡先の管理 ユーザの履歴 Cisco Jabber のサポート 複数のクライアント デバイスのサポート：Microsoft windows、MAC、Mobile、タブレット、IOS、Android、BB Microsoft Office の統合 LDAP directory integration 個人用ディレクトリおよび友人リスト オープン API システム トラブルシューティング		Cisco テレフォニーのアベイラビリティ Microsoft Outlook カレンダーの統合（オンプレミスの Exchange あるいは ホスト型 Office 365 展開）	リモート Cisco IP Phone 制御 リモート ソフトフォン 制御

コア IM とアベイラビリティ機能	高度な IM 機能（オプション）	豊富な Unified Communications アベイラビリティ機能（オプション）	リモート デスク フォン制御（オプション）
	常設チャット マネージド ファイル転送 メッセージ アーカイバ サードパーティのカレンダー XMPP クライアントのサポート 高可用性 拡張性：WAN 経由のマルチノード サポートおよびクラスタリング クラスタ間ピアリング エンタープライズとの連携： • IM and Presence Service の統合 • Cisco Webex Messenger の統合 • Microsoft Business/Office365 向け Lync/Skype for Business の統合 • IBM SameTime の統合 • Cisco Jabber XCP パブリック フェデレーション： • Google Talk、AOL の統合 • XMMP サービスまたは BOT • サードパーティの Exchange サービスの統合 IM コンプライアンス SAML シングル サインオン		

コア IM とアベイラビリティ機能	高度な IM 機能（オプション）	豊富な Unified Communications アベイラビリティ機能（オプション）	リモート デスク フォン制御（オプション）
	カスタム ログイン バナー		

標準導入 vs 中央クラスタ

システムをインストールする前に、まず、IM and Presence Service の標準の導入を展開するか、現状のトポロジおよびインストールへの影響を鑑みて、IM and Presence Service の中央クラスタを採用するかを決定する必要があります。

- Cisco Unified Communications Manager（標準展開）上の IM and Presence Service： 標準の展開では、IM and Presence Service クラスタが、Cisco Unified Communications Manager のテレフォニー ノードと同じサーバにインストールされます。IM and Presence クラスタは、プラットフォームと多くのテレフォニー クラスタと同じサービスを共有します。このオプションでは、IM and Presence クラスタへのテレフォニー クラスタの 1 x 1 のマッピングが必要です。
- 集中 IM and Presence スクラスタ： この導入方法では、IM and Presence Service クラスタがテレフォニークラスタから独立してインストールされます。トポロジの計画方法によっては、IM and Presence の中央クラスタをテレフォニー クラスタとは全く別の複数の物理ハードウェア サーバにインストールすることができます。この導入オプションでは、テレフォニー クラスタと IM and Presence クラスタの 1 対 1 のマッピング要件が削除され、それぞれの展開の種類をニーズに応じて適切に拡張できます。

（注） IM and Presence クラスタには、Cisco Unified Communications Manager のインスタンスが継続して含まれます。ただし、このインスタンスは、ユーザのプロビジョニングおよびデータベースを処理するためのもので、テレフォニーを処理するものではありません。テレフォニー統合については、IM and Presence の中央クラスタは、別の Unified Communictions Manager テレフォニークラスタに接続する必要があります。

このドキュメントの手順は、標準の展開および中央クラスタ展開の両方で利用することができます。ただし、中央クラスタを展開する場合は、「集中展開の設定 （115 ページ）」のタスクも完了して、テレフォニー クラスタと IM and Presence クラスタを適切に配置する必要があります。

マルチノードの拡張性機能

マルチノードの拡張性要件

IM and Presence サービスはマルチノードの拡張性をサポートします。

- クラスタあたり 6 個のノード
- 完全な Unified Communication（UC）モード展開でノードごとに最大 25,000 ユーザを持つクラスタあたり 75,000 ユーザ
- プレゼンス冗長グループでクラスタあたり 25,000 ユーザ、およびハイ アベイラビリティの展開でクラスタあたり 75,000 ユーザ。
- ユーザあたりの最大連絡先の管理可能なカスタマー定義制限（デフォルトは無制限）
- IM and Presence サービスはマルチノード機能をもつクラスタ間展開をサポートしています。

OVA 要件

以下の OVA 要件が適用されます。

- 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。
- 常設チャットの展開には、少なくとも15,000 ユーザ OVA を導入することを推奨します。
- 中央集中型の導入の場合は、最小 OVA 15,000 ユーザと、25,000 ユーザ IM and Presence OVA を推奨します。15,000ユーザ OVA は、25000ユーザにまで拡張できます。25K OVA テンプレートと高可用性を有効にした 6 ノード クラスタでは、IM and Presence サービスの中央展開で最大 75,000 のクライアントをサポートしています。25K OVA で 75K ユーザをサポートするには、XCP ルータのデフォルト トレース レベルを **[情報（Info）]** から **[エラー（Error）]** に変更する必要があります。中央クラスタの Unified Communications Manager パブリッシャ ノードでは、次の要件が適用されます。
  - 25000 IM and Presence OVA (最大75000ユーザ) は、中央クラスタの Unified Communications Manager パブリッシャ ノードにインストールされた1万ユーザ OVA を使用して展開できます。
  - 15000 IM and Presence OVA (最大45,000ユーザ) は、中央クラスタの Unified Communications Manager パブリッシャ ノードにインストールされた 7500 ユーザ OVA を使用して展開できます。

（注） Multiple Device Messaging を有効にする場合は、各ユーザが複数の Jabber クライアントを持つ可能性があるため、ユーザ数ではなくクライアント数に応じた展開にします。たとえば、ユーザ数が 25,000 人で、各ユーザが 2 台の Jabber クライアントを保持している場合、導入環境には 5 万ユーザのキャパシティが必要となります。

拡張性は、展開内のクラスタの数によって異なります。VM の設定要件および OVA テンプレートの詳細は、以下の URL の *Virtualization for Unified CM IM and Presence* を参照してください。

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html

展開の拡張性オプション

IM and Presence Service クラスタは、最大 6 台のノードをサポートできます。最初に 6 台未満のノードをインストールした場合は、追加ノードをいつでもインストールできます。より多くのユーザをサポートするために IM and Presence 展開を拡張する場合、設定したマルチノード展開モデルを考慮する必要があります。次の表で、各マルチノード展開モデルの拡張性オプションについて説明します。

表 3:

構成モード	拡張性オプション	
	既存のプレゼンス冗長グループへの新しいノードの追加	新しいプレゼンスへの新規ノードの追加 冗長グループ
平衡型非冗長ハイアベイラビリティ展開	既存のプレゼンス冗長グループに新しいノードを追加すると、新しいノードが既存のノードと同じ数のユーザをサポートできます。プレゼンス冗長グループは、ユーザの数の2倍をサポートできます。また、そのプレゼンス冗長グループ内の既存のノードと新しいノードのユーザに平衡型ハイアベイラビリティを提供します。	新しいプレゼンス冗長グループに新しいノードを追加すると、展開でより多くのユーザをサポートできます。 これはプレゼンス冗長グループ内のユーザに平衡型ハイアベイラビリティを提供しません。平衡型ハイアベイラビリティを実現するには、プレゼンス冗長グループに2番目のノードを追加する必要があります。

構成モード	拡張性オプション	
	既存のプレゼンス冗長グループへの新しいノードの追加	新しいプレゼンスへの新規ノードの追加 冗長グループ
平衡型冗長ハイ アベイラビリティ展開	既存のプレゼンス冗長グループに新しいノードを追加すると、新しいノードが既存のノードと同じユーザをサポートできます。たとえば、既存のノードが5,000 人のユーザをサポートする場合、新しいノードは同じ5,000 人のユーザをサポートします。また、そのプレゼンス冗長グループ内の既存のノードと新しいノードのユーザに平衡型冗長ハイアベイラビリティを提供します。 （注） 既存のノード上のユーザ数に応じて、プレゼンス冗長グループ内でのユーザの再割り当てが必要になることがあります。	新しいプレゼンス冗長グループに新しいノードを追加すると、展開でより多くのユーザをサポートできます。 これはプレゼンス冗長グループ内のユーザに平衡型ハイアベイラビリティを提供しません。平衡型ハイアベイラビリティを実現するには、プレゼンス冗長グループに2番目のノードを追加する必要があります。
アクティブ/スタンバイ冗長ハイ アベイラビリティ展開	既存のプレゼンス冗長グループに新しいノードを追加すると、プレゼンス冗長グループの既存のノードのユーザにハイアベイラビリティが提供されます。これは、ハイアベイラビリティ拡張機能だけを提供します。展開でサポートできるユーザ数は増えません。	新しいプレゼンス冗長グループに新しいノードを追加すると、展開でより多くのユーザをサポートできます。 これはプレゼンス冗長グループ内のユーザにハイアベイラビリティを提供しません。ハイアベイラビリティを実現するには、プレゼンス冗長グループに2番目のノードを追加する必要があります。

WAN の導入

IM and Presence Service は、クラスタ内およびクラスタ間での WAN 経由のクラスタリング展開をサポートします。このオプションでは、導入環境に地理的冗長性を追加することができます。

WAN 経由のクラスタ内展開

IM and Presence Service では、このモジュールに記載された推奨帯域幅を使用した WAN 経由のクラスタ内展開をサポートしています。IM and Presence Service では、プレゼンス冗長グループ内の 1 つのノードが 1 つの地理的なサイトに存在し、プレゼンス冗長グループ内の 2 番目のノードが別の地理的な場所にあるような、WAN 上で地理的に分割された単一のプレゼンス冗長グループをサポートします。

このモデルは、地理的冗長性およびリモート フェールオーバー（たとえば、リモート サイトのバックアップ IM and Presence Service ノードへのフェールオーバー）を提供できます。このモデルでは、IM and Presence Service ノードを Cisco Unified Communications Manager データベース パブリッシャ ノードと共存させる必要はありません。Cisco Jabber クライアントは、IM and Presence Service ノードに対してローカルまたはリモートからアクセスできます。

このモデルは、クライアントのハイ アベイラビリティをサポートし、サービスまたはハードウェアがホームの IM and Presence Service ノードで失敗した場合、クライアントはリモート ピアの IM and Presence Service ノードにフェールオーバーします。障害が発生したノードが再度オンラインになると、クライアントはホームの IM and Presence Service ノードに自動的に再接続します。

WAN 経由でリモート フェールオーバーを備えた IM and Presence Service を展開する場合は、次の制約事項に注意してください。

- このモデルは、システム レベルのハイ アベイラビリティのみをサポートします。特定の IM and Presence Service コンポーネントに、シングル ポイント障害が存在する場合があります。これらのコンポーネントは、Cisco Sync Agent、Cisco Intercluster Sync Agent、および Cisco Unified CM IM and Presence の管理インターフェイスです。

IM and Presence Service は、WAN 経由のクラスタリング展開において複数のプレゼンス冗長グループをサポートします。WAN 経由のクラスタリング展開の規模については、IM and Presence Service SRND を参照してください。

詳細については、*IM and Presence Service* ソリューション リファレンス ネットワーク デザイン（SRND）を参照してください。

WAN 経由の展開のマルチノード設定

WAN 経由のクラスタ内展開用に IM and Presence Service のマルチノード機能を設定する場合は、マルチノードの項で説明するように IM and Presence Service プレゼンス冗長グループ、ノード、およびユーザ割り当て設定します。ただし、次の推奨事項に注意してください。

- 最適なパフォーマンスを得るため、ホームの IM and Presence Service ノードにユーザの大部分を割り当てることを推奨します。この展開モデルでは、WAN 経由でリモート IM and Presence

Service ノードに送信されるメッセージの量が少なくなりますが、セカンダリ ノードへのフェールオーバー時間は、フェールオーバーするユーザの数によって異なります。

- WAN 経由のハイ アベイラビリティ展開モデルを設定する場合は、プレゼンス冗長グループ全体の DNS SRV アドレスを設定できます。この場合、IM and Presence Service は、DNS SRV で指定されたノードへの最初の PUBLISH 要求メッセージを送信し、応答メッセージは、ユーザのホスト ノードを示します。IM and Presence Service はホスト ノードにそのユーザに対する後続の PUBLISH メッセージをすべて送信します。このハイ アベイラビリティの展開モデルを設定する前に、WAN 経由で送信される可能性があるメッセージの量に十分な帯域幅があるかどうかを検討する必要があります。

WAN 経由のクラスタ間展開

IM and Presence Service では、このモジュールに記載された推奨帯域幅を使用した WAN 経由のクラスタ間展開をサポートしています。クラスタ間の展開を導入する場合は、以下の点に注意します。

- クラスタ間ピアと呼ばれる、スタンドアロンの IM and Presence Service クラスタを相互接続するピア関係を設定することができます。このクラスタ間ピアの機能を使用すると、ある IM and Presence Service クラスタ内のユーザは、同じドメイン内のリモート IM and Presence Service クラスタのユーザのアベイラビリティ情報を通信およびサブスクライブできます。クラスタ間ピアの設定方法の詳細は、「クラスタ間ピアの設定（187ページ）」を参照してください。
- ノード名：任意の IM and Presence Service ノードに定義したノード名は、すべてのクラスタ内の他のすべての IM and Presence Service ノードで解決可能でなければなりません。したがって、各 IM and Presence Service ノード名はノードの FQDN である必要があります。ネットワークに DNS が展開されていない場合は、各ノード名が IP アドレスである必要があります。
- IM アドレス スキーム：クラスタ間展開の場合、各クラスタ内のすべてのノードは同じ IM アドレス スキームを使用する必要があります。あるクラスタ内のいずれかのノードが、Release 10 以前のあるバージョンの IM and Presence Service を実行している場合、下位互換性のために、すべてのノードが UserID@Default_Domain の IM アドレス スキームを使用するように設定する必要があります。
- ルータ間通信：デフォルト設定では、IM and Presence Service は、クラスタ間のルータ間コネクタとしてクラスタ内のすべてのノードを割り当てます。IM and Presence Service は、AXL インターフェイスを介してクラスタ間にクラスタ間ピア接続を確立すると、ホームおよびリモート クラスタのすべてのクラスタ間ルータツールータ コネクタ ノードからの情報を同期化します。

  また、TLS を使用したルーター間のセキュアな通信を設定して、ローカル クラスタ内の各ルータ間コネクタ ノードおよびリモート クラスタ内の各ルータ コネクタ ノード間の接続を保護することも可能です。

SAML シングル サインオンの展開

Security Assertion Markup Language（SAML）シングル サインオン機能を使用すると、管理ユーザは以下のいずれかのアプリケーションサインインした後、 IM and Presence Serviceを含め、数多くの Cisco Collaboration アプリケーションにアクセスすることができます。この機能は、以下の方法で管理者のジョブを簡素化します。

- シングル サインイン後に、数多くの Cisco Collaboration アプリケーションにアクセスするには、単一のログインが必要となります。
- 必要なパスワードは 1 つのみで、アプリケーション毎に異なるパスワードを覚える必要はありません。
- 管理者は、すべてのパスワードと認証を単一の ID プロバイダー (IdP) で管理することができます。

SAML シングル サインオンのセットアップおよび設定の詳細は、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*Cisco Unified Communications Solutions* 向け *SAML SSO* 導入ガイド』を参照してください。

サードパーティ統合

IM and Presence Service は、さまざまなサードパーティ システムと統合されています。以下の表に、統合の概要と、その構成方法を説明したドキュメントへのリンクが提供されています。

マニュアルのタイトル	このマニュアルの構成
IM and Presence サービス 向け Microsoft Outlook 予定表統合ガイド	IM and Presence Service を設定し、オンプレミスの Microsoft Exchange サーバ あるいはホスト型の Office 365 サーバに接続して、IM and Presence Servic ユーザのプレゼンス ステータスに Microsoft Outlook のカレンダー情報を使用します。

マニュアルのタイトル	このマニュアルの構成
IM and Presence Service 向けドメイン間連携	IM and Presence Service を設定して、以下のシステムとのドメイン間連携を行います。この設定で、IM and Presence ユーザが、他のシステム上のユーザと IM および プレゼンスの情報を交信することができます。 • Microsoft Lync[MicrosoftLync] • Microsoft Skype for Business • Microsoft Office 365 • GoogleTalk • AOL • IBM Sametime • Cisco Webex Messenger • 別の IM and Presence Service エンタプライズ
IM and Presence Service のパーティション化されたドメイン間連携	Microsoft Lync または Skype for Businessとのパーティション化されたドメイン間連携用にIM and Presence Service を設定します。この統合によって、ユーザの IM and Presence Service への移行中でも、ネットワーク内の通信を維持することができます。

サードパーティのクライアントの統合

このセクションでは、サードパーティのクライアントの統合に関する要件の概要について説明します。

サポートされているサードパーティ製 XMPP クライアント

IM and Presence Service は、アベイラビリティおよびインスタントメッセージ（IM）サービスのためにサードパーティ製 XMPP クライアント アプリケーションを IM and Presence Service と統合できるように、標準ベースの XMPP をサポートしています。サードパーティ製 XMPP クライアントが、Cisco ソフトウェア開発キット（SDK）にある標準ベースの XMPP に準拠している必要があります。

このモジュールでは、XMPP クライアントを IM and Presence Service と統合するための設定要件について説明します。XMPP ベースの API（Web）クライアントアプリケーションを IM and Presence Service と統合する場合は、Cisco Developer ポータルにある IM and Presence Service の開発者マニュアルを参照してください。

http://developer.cisco.com/

ライセンス要件

XMPP クライアント アプリケーションのユーザごとに IM and Presence Service 機能を割り当てる必要があります。IM and Presence 機能は、User Connect Licensing（UCL）と Cisco Unified Workspace Licensing（CUWL）の両方に含まれています。

ライセンスの詳細は、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある『*Cisco Unified Communications Manager*システム設定ガイド』の「スマート ソフトウェア ライセンシング」の章を参照してください。

Cisco Unified Communications Manager での XMPP クライアント統合

XMPP クライアントを統合する前に、Cisco Unified Communications Manager で次のタスクを実行します。

- ライセンス要件を設定します。
- ユーザとデバイスを設定します。デバイスを各ユーザに関連付け、ユーザをライン アピアランスに関連付けます。

XMPP 連絡先検索のための LDAP 統合

XMPP クライアント アプリケーションのユーザがサードパーティ LDAP ディレクトリから連絡先を検索および追加できるようにするには、IM and Presence Service で XMPP クライアントの LDAP 設定を実行します。

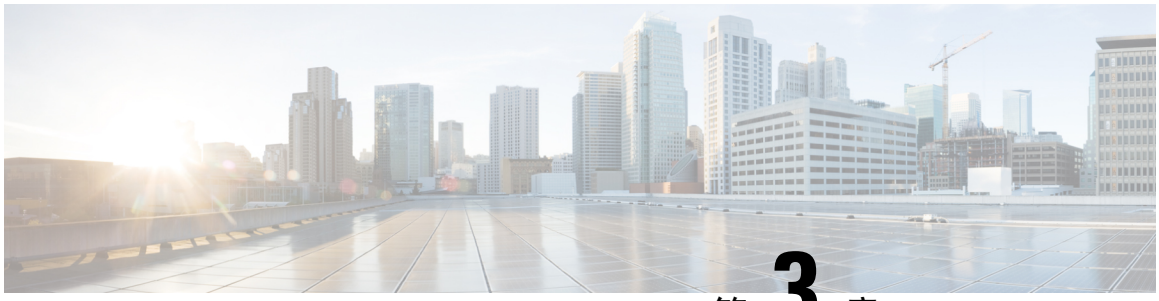
XMPP クライアントの DNS 設定

XMPP クライアントを IM and Presence Service と統合する場合は、展開内の DNS SRV を有効にする必要があります。XMPP クライアントは、DNS SRV クエリーを実行して、通信する XMPP ノード（IM and Presence Service）を検索し、XMPP ノードのレコードルックアップを実行して IP アドレスを取得します。

（注） IM and Presence Service の展開で複数の IM ドメインを設定した場合は、各ドメインに DNS SRV レコードが必要です。すべての SRV レコードは、同じ結果セットに解決できます。

第 II 部

システムを設定する



第 3 章

ドメインを設定する

ドメイン設定の概要

IM and Presence Domain ウィンドウに以下のドメインの種類が表示されます。

- 管理者が管理する IM アドレス ドメイン。これらは、手動で追加されたが、どのユーザにも割り当てられていない内部ドメインか、Sync Agent によって自動的に追加されたが、その後でユーザのドメインが変更されたために使用されていない内部ドメインです。
- システムが管理する IM アドレス ドメイン。これらは、ユーザが展開で使用し、手動または自動のいずれでも追加できる内部ドメインです。

ドメインが [IM and Presence ドメイン（IM and Presence Domain）] ウィンドウに表示されている場合は、ドメインは有効になっています。ドメインを有効化する必要はありません。ローカルI IM アドレス ドメインは、手動で追加、更新、削除が可能です。

2 個のクラスタでドメインを設定することはできますが、ピア クラスタのみで使用されている場合に限ります。これは、ローカル クラスタのシステムが管理するドメインとして表示されますが、ピア クラスタで使用中であると識別されます。

CiscoSync Agent サービスが夜間監査を実行し、ローカル クラスタ、およびクラスタ間が設定されている場合はピア クラスタの各ユーザのディレクトリ URI を確認して、一意のドメインのリストを自動的に構築します。クラスタ内のユーザがそのドメインに割り当てられると、管理者管理ドメインからシステム管理ドメインに変更されます。クラスタ内のユーザがドメインを使用しなくなった場合は、ドメインは管理者管理のドメインに戻ります。

ドメイン設定例

Cisco Unified Communications Manager IM and Presence サービスは、任意の数の DNS ドメインへの柔軟なノード展開をサポートします。この柔軟性をサポートするには、展開内のすべての IM and

Presence サービス ノードにそのノードの完全修飾ドメイン名（FQDN）に設定されたノード名が必要です。以下の IM and Presence Service 向けノード展開オプションの例を説明します。

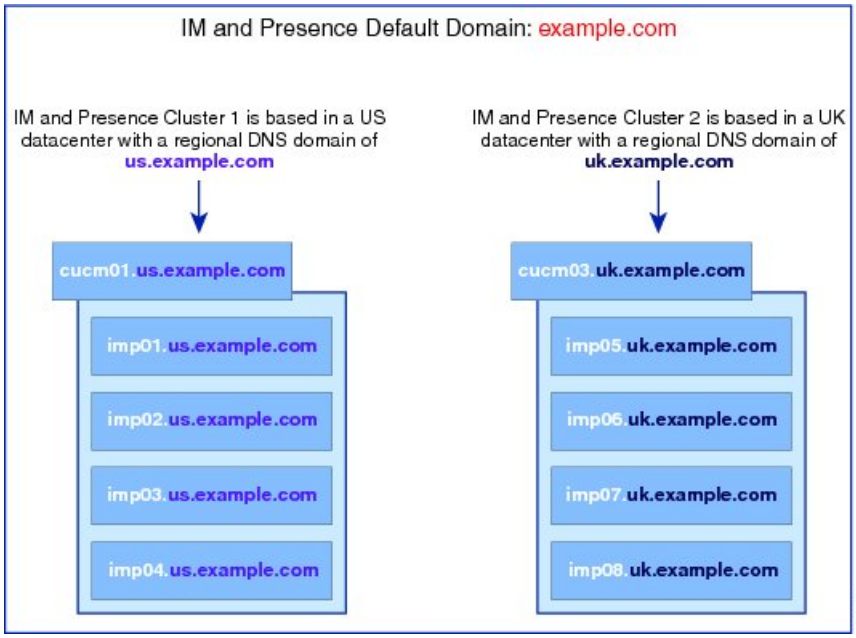
- 別々の DNS ドメインおよびサブドメインを持つ複数の DNS ドメイン
- 別々の DNS ドメインおよびサブドメインを持つ単一クラスタ
- DNS ドメインが Unified Communications Manager のドメインと異なる単一クラスタ

（注） ある IM and Presence サービス ノード名がホスト名だけに基づいている場合、すべての IM and Presence サービス ノードが同じ DNS ドメインを共有する必要があります。

システムによって、IM and Presence サービス のデフォルト ドメインまたは DNS ドメインと一致するように設定される他の IM ドメインは必要はありません。IM and Presence サービス展開に共通のプレゼンス ドメインを配置し、ノードを複数の DNS ドメインに展開することができます。

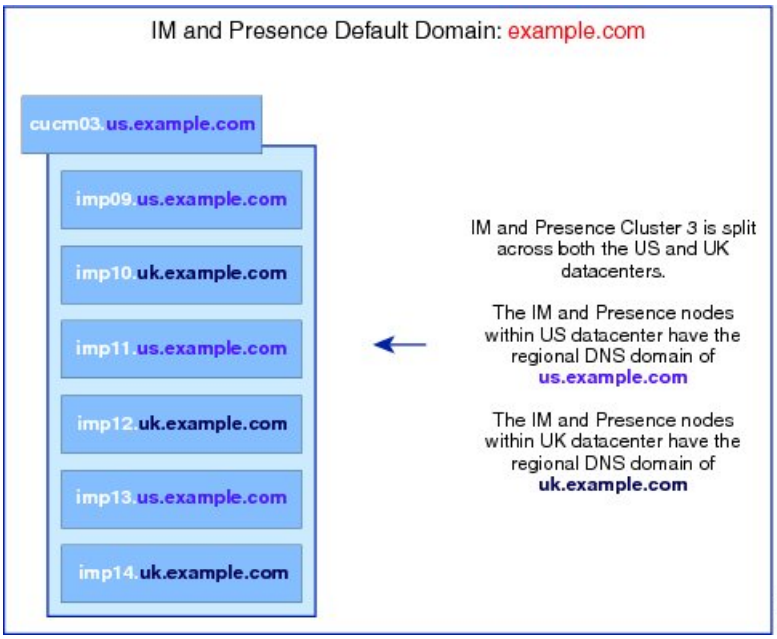
別々の DNS ドメインおよびサブドメインを持つ複数の DNS ドメイン

IM and Presence Service は、ピアの IM and Presence Service クラスタを構成するノードとは異なる DNS ドメインまたはサブドメイン内の 1 つの IM and Presence Service クラスタに関連付けられたノードをサポートします。次の図に、サポートされている展開シナリオの例を示します。



別々の DNS ドメインおよびサブドメインを持つ単一クラスタ

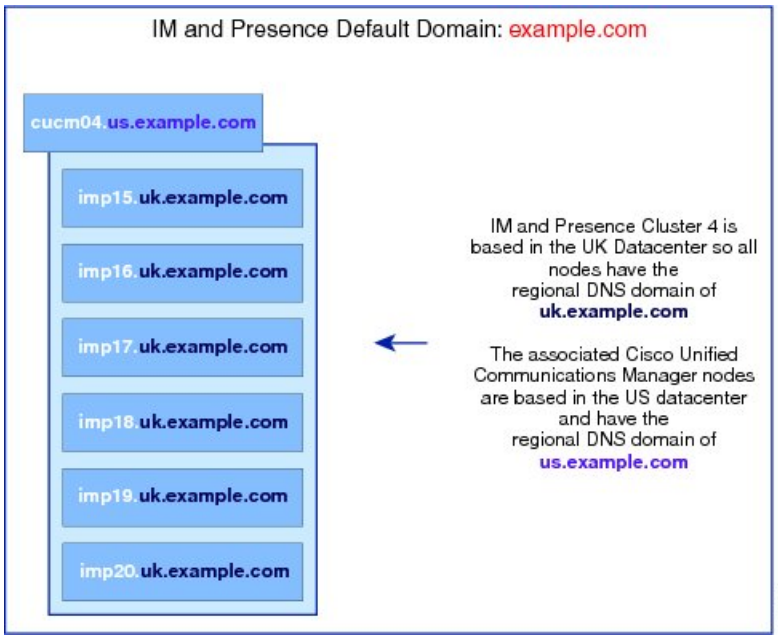
IM and Presence Service は、複数の DNS ドメインまたはサブドメインに展開された IM and Presence Service クラスタ内へのノードの配置をサポートします。次の図に、サポートされている展開シナリオの例を示します。



（注） ハイ アベイラビリティは、プレゼンス冗長グループ内の 2 台のノードが別々の DNS ドメインまたはサブドメインにあるシナリオでも完全にサポートされます。

DNS ドメインが Unified Communications Manager のドメインと異なる単一クラスタ

IM and Presence Service は、関連する Cisco Unified Communications Manager クラスとは異なる DNS ドメインへの IM and Presence Service ノードの配置をサポートします。次の図に、サポートされている展開シナリオの例を示します。



（注） Cisco Unified Communications Manager とのアベイラビリティ統合をサポートするには、**CUCM Domain** の SIP Proxy サービス パラメータが Cisco Unified Communications Manager クラスタの DNS ドメインと一致する必要があります。

デフォルトでは、このサービス パラメータは IM and Presence データベース パブリッシャ ノードの DNS ドメインに設定されています。IM and Presence データベース パブリッシャ ノードの DNS ドメインが Cisco Unified Communications Manager クラスタの DNS ドメインと異なる場合、Cisco Unified Communications Manager のドメインを使用するようにこのサービス パラメータを編集する必要があります。

ドメイン要件を設定する

- この機能を使用するには、IM and Presence Service および Cisco Unified Communications Manager のすべてのノードおよびクラスタが複数のドメインをサポートする必要があります。IM and Presence Service クラスタ内のすべてのノードが Release 10.0 以降を使用して実行していることを確認します。
- アドレス用ディレクトリ URI が設定されていることを確認します。詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある『*Cisco Unified Communications Manager* システム設定ガイド』の「URI ダイヤリングの設定」を参照してください。

ドメインのタスクフローを設定する

IM and Presence Service 向けにドメインを設定するには、このタスクを完了します。

手順

	コマンドまたはアクション	目的
Step 1	ハイ アベイラビリティを無効にする （30 ページ）	[ハイ アベイラビリティ] が有効化されている場合は、無効にします。デフォルト ドメインを変更する場合は、一時的にサービスを停止する必要があります。ハイ アベイラビリティが有効のままサービスを停止すると、システム フェールオーバーが発生します。
Step 2	IM and Presence Services の無効化 （30 ページ）	ドメインを変更する前に、重要なサービスを停止させます。
Step 3	IM and Presence Service のデフォルト ドメインを設定する （32 ページ）	IM and Presence Service クラスタ のデフォルト ドメインの値を設定します。この手順は、DNS および非 DNS 展開で適用可能です。
Step 4	以下のタスクを実行します。 • IM アドレス ドメインを追加または更新する （33 ページ） • IM アドレス ドメインを削除する （34 ページ）	オプション。ローカル クラスタの管理者管理のドメインを追加、編集、削除するときのみ、このタスクを実行します。
Step 5	XMPP クライアントおよび TLS 証明書を再生成する （35 ページ）	TLS XMPP 連携を使用している場合、新しい XMPP クライアントおよび TLS 証明書を生成する手順に進みます。
Step 6	IM and Presence Services を起動する （35 ページ）	ドメインの設定が完了したら、サービスを再起動します。
Step 7	プレゼンス冗長グループに対するハイアベイラビリティを有効にする （36 ページ）	ハイ アベイラビリティが設定されていた場合、再度有効にします。 （注） ハイ アベイラビリティを有効にする前に、再起動したサービスがすべてのクラスタ ノードで稼働しているかを確認します。

ハイ アベイラビリティを無効にする

ハイ アベイラビリティが設定されている場合、デフォルト ドメインを設定する前に、各プレゼンス冗長グループにおいてハイ アベイラビリティを無効にしなければなりません。デフォルト ドメインのサービスを停止する際に、ハイ アベイラビリティが有効になっている場合、フェイルオーバーが発生します。

（注） [プレゼンス冗長グループの詳細（**Presence Redundancy Group Details**）] ページには、クラスタで高可用性が無効になっている場合でも、すべてのアクティブな JSM セッションが表示されます。

始める前に

各プレゼンス冗長グループの各クラスタ ノードのアクティブ ユーザ数を記録します。この情報は、Cisco Unified CM IM and Presence の（**System** > **Presence Topology**）ウィンドウに表示されます。この番号は、後にハイ アベイラビリティを再度有効にする際に必要となります。

手順

Step 1 Cisco Unified CM Administration のユーザ インターフェイスから、**[システム（System）] > [プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。

Step 2 **検索**をクリックして、グループを選択します。

Step 3 [プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウで、**[ハイ アベイラビリティを有効にする（Enable High Availability）]** チェックボックスをオフにします。

Step 4 [保存（Save）] をクリックします。

Step 5 各プレゼンス冗長グループに対して、この手順を繰り返します。

Step 6 完了後、さらに変更を行う前に、新しい HA 設定がクラスタ全体にわたって同期されるまで、少なくとも 2 分待機します。

次のタスク

IM and Presence Services の無効化 （30 ページ）

IM and Presence Services の無効化

この手順を使用して、デフォルト ドメインに変更を加える前に、IM and Presenceのサービスを停止します。クラスタ内のすべてのノードでこの手順を実行します。

始める前に

ハイアベイラビリティが無効になっていることを確認します。詳細については、「ハイアベイラビリティを無効にする （30 ページ）」を参照してください。

手順

Step 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-ネットワークサービス（Control Center - Network Services）]** を選択します。

Step 2 [サーバ（Server）] リストから、サービスを非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。

Step 3 **IM and Presence Services** のエリアで、以下のサービスが開始されていることを確認します。

- **Cisco Client Profile Agent**
- **Cisco Sync Agent**
- **Cisco XCP Router**

Step 4 [Stop] をクリックします。

Step 5 [関連リンク（Related Links）] ドロップダウン リストから [サービスのアクティブ化（Service Activation）] を選択し、[移動（Go）] をクリックします。

Step 6 **IM and Presence Services** のエリアで、以下のサービスが開始されていることを確認します。

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

Step 7 [保存（Save）] をクリックします。

Step 8 これらのサービスを無効にしたすべてのノードのリストを作成します。デフォルト ドメインの変更が完了したら、サービスを再起動する必要があります。

次のタスク

IM and Presence Service のデフォルト ドメインの設定：

- IM and Presence Service のデフォルトドメインを設定する （32 ページ）

あるいは、デフォルト ドメインがすでに設定されている場合、このタスクのいずれかを使って、ドメインの追加または削除を行います。

- IM アドレスドメインを追加または更新する （33 ページ）
- IM アドレスドメインを削除する （34 ページ）

IM and Presence Service のデフォルトドメインを設定する

この手順を使って、IM and Presence Service クラスタ のデフォルト ドメインの値を設定します。DNS または非 DNS 展開が存在する場合、この手順を適用できます。

この手順では、IM and Presence Service のクラスタのデフォルト ドメインだけを変更します。そのクラスタ内のすべての IM and Presence サービス ノードに関連付けられている DNS ドメインは変更されません。IM and Presence Service ノードの DNS ドメインを変更する方法の手順については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlの *Cisco Unified Communications Manager* および *IM and Presence Service* の *IP* アドレスおよびホスト名の変更 を参照してください。

（注） Cisco Unified Communications Manager に IM and Presence Service パブリッシャのノードを追加すると、デフォルト ドメインが設定されます。ノードのインストール中、Cisco Unified Communications Manager からデフォルト ドメイン 値が取得できない場合、デフォルト ドメイン値は「DOMAIN.NOT.SET（DOMAIN.NOT.SET）」にリセットされます。IM and Presence Service のデフォルト ドメイン値を有効なドメイン値に変更するには、この手順を使用します。

始める前に

ハイ アベイラビリティが無効になっていて、重要なIM and Presence Services が停止されていることを確認します。詳細は、「IM and Presence Services の無効化 （30 ページ）」を参照してください。

手順

Step 1 IM and Presence Service のパブリッシャ ノードにログインします。

Step 2 **Cisco Unified CM IM and Presence 管理**で **プレゼンス** > **設定** > **詳細設定** を選択します。

Step 3 **[デフォルト ドメイン（Default Domain）]** を選択します。

Step 4 **[ドメイン名（Domain Name）]** フィールドに、新しいプレゼンス ドメインを入力し、**[保存（Save）]** を選択します。

システム アップデートは完了まで最長で 1 時間かかる場合があります。アップデートに失敗すると、**[再試行（Re-try）]** ボタンが表示されます。変更を再適用するには、**[再試行（Re-try）]** をクリックします。または **[取消（Cancel）]** をクリックします。

次のタスク

TLS XMPP 連携を使用している場合、「XMPP クライアントおよび TLS 証明書を再生成する （35 ページ）」に進みます。

IM アドレスドメインを追加または更新する

管理者管理のドメインをローカル クラスタ上に追加または編集することができます。別のクラスタに関連付けられたシステム管理ドメインまたは管理者によって管理されるドメインは編集できません。

システム管理ドメインが使用中であるため、編集できません。その IM アドレス ドメインのシステムにユーザが存在しない場合（たとえば、ユーザが削除された場合）、システム管理ドメインは自動的に管理者の管理ドメインになります。管理者の管理ドメインは編集または削除できます。

始める前に

ハイ アベイラビリティが無効になっていて、重要なIM and Presence Services が停止されていることを確認します。詳しくは「IM and Presence Services の無効化 （30 ページ）」を参照してください。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**プレゼンス** > > **ドメイン**を選択します。

すべての管理者の管理 IM アドレス ドメインとシステム管理 IM アドレス ドメインを表示する [ドメインの検索と一覧（Find and List Domains）] ウィンドウが表示されます。

Step 2 次のいずれかの操作を実行します。

- [新規追加（Add New）] をクリックすることで、新しいドメインを追加します。[ドメイン（Domains）] ウィンドウが表示されます。
- ドメインのリストから編集するドメインを選択します。[ドメイン（Domains）] ウィンドウが表示されます。

Step 3 最大 255 文字の一意なドメイン名を [ドメイン名（Domain Name）] フィールドに入力し、[保存（Save）] をクリックします。

各ドメイン名は、クラスタ内で一意である必要があります。指定できる値は、すべての大文字または小文字（a-zA-Z）、すべての番号（0-9）、ハイフン（-）、またはドット（.）です。ドメイン ラベルの区切り文字はドットです。ドメイン ラベルの先頭文字をハイフンにすることはできません。最後のラベル（たとえば、.com）の先頭文字を数字にすることはできません。たとえば、Abc.1om は無効なドメインです。

次のタスク

TLS XMPP 連携を使用している場合、「XMPP クライアントおよび TLS 証明書を再生成する （35 ページ）」に進みます。

IM アドレスドメインを削除する

Cisco Unified CM IM and Presence の管理 GUI を使用して、ローカル クラスタにある管理者の管理 IM アドレス ドメインを削除できます。

システム管理のドメインは使用中であるため、削除できません。その IM アドレス ドメインのシステムにユーザが存在しない場合（たとえば、ユーザが削除された場合）、システム管理ドメインは自動的に管理者の管理ドメインになります。管理者の管理ドメインは編集または削除できます。

（注） ローカルクラスタとピアクラスタの両方に設定された管理者の管理ドメインを削除すると、ドメインは管理者の管理ドメインのリストに保持されます。ただし、そのドメインはピア クラスタでのみ設定済みとマークされます。完全にエントリを削除するには、設定されたすべてのクラスタからドメインを削除する必要があります。

始める前に

ハイ アベイラビリティが無効になっていて、重要なIM and Presence Services が停止されていることを確認します。詳細は、IM and Presence Services の無効化 （30 ページ）を参照してください。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**プレゼンス** > **ドメイン**を選択します。

すべての管理者管理の IM アドレス ドメインおよびシステム管理 IM アドレス ドメインを表示する **ドメインの検索/一覧表示** ウィンドウが表示されます。

Step 2 次の方法の 1 つを使用して削除する管理者の管理ドメインを選択し、次に [選択項目の削除（Delete Selected）] をクリックします。

- 削除するドメインの横のチェックボックスをオンにします。
- 管理者の管理ドメインのリストのドメインをすべて選択するには、**[すべてを選択（Select All）]** をクリックします。

ヒント すべての選択をクリアするには、[すべてをクリア（Clear All）] をクリックします。

Step 3 [OK] をクリックして削除を確定するか、[取消（Cancel）] をクリックします。

次のタスク

TLS XMPP 連携を使用している場合、「XMPP クライアントおよび TLS 証明書を再生成する （35 ページ）」に進みます。

XMPP クライアントおよび TLS 証明書を再生成する

IM ドメインに変更を加えたら、XMPP クライアントまたは TLS 証明書を再生成する必要があります。

手順

Step 1 **Cisco Unified CM IM and Presence OS 管理**で、**セキュリティ** > **証明書管理**を選択します。

Step 2 **検索**をクリックして、証明書の一覧を開きます。

Step 3 **cup-xmpp-s2s**証明書をクリックします。

Step 4 **証明書の詳細**ウィンドウで、**再生成**をクリックします。

IM and Presence Services を起動する

デフォルト ドメインに変更を加えた後、この手順で、すべてのクラスタ ノード上で IM and Presence サービスを再起動します。

始める前に

XMPP クライアントおよび TLS 証明書を再生成する （35 ページ）

手順

Step 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-ネットワークサービス（Control Center - Network Services）]** を選択します。

Step 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。

Step 3 **IM and Presence Services** のエリアで、以下のサービスを選択します。

- **Cisco Client Profile Agent**
- **Cisco Sync Agent**
- **Cisco XCP Router**

Step 4 [再起動（Restart）] をクリックします。

Step 5 [関連リンク（Related Links）] ドロップダウン リストから [サービスのアクティブ化（Service Activation）] を選択し、[移動（Go）] をクリックします。

Step 6 **IM and Presence Services** のエリアで、以下のサービスを選択します。

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

Step 7 [保存（Save）] をクリックします。

次のタスク

プレゼンス冗長グループに対するハイアベイラビリティを有効にする （36 ページ）

プレゼンス冗長グループに対するハイアベイラビリティを有効にする

デフォルト ドメインを変更し、IM and Presence サービスを再起動した後で、プレゼンス冗長グループのハイ アベイラビリティを有効にすることができます。

始める前に

ハイ アベイラビリティを有効化する前に、すべてのサービスが IM and Presence データベース パブリッシャ ノードおよびサブスクライバ ノードで稼働していなければなりません。サービスが再起動してから30分以内の場合は、ハイ アベイラビリティを有効にする前に Cisco Jabber セッションが再作成されたことを確認します。十分な時間を確保しない場合、セッションが作成されていない Jabber クライアントでプレゼンスは機能しません。

Cisco Jabber セッションの数を取得するには、すべてのクラスタ ノードで `show perf query counter "Cisco Presence Engine" Active JsmSessions` CLI コマンドを実行します。アクティブ セッションの数は、ハイ アベイラビリティを無効にした際に記録したユーザ数と一致するはずです。

次の段階で、パブリッシャとサブスクライバの両方でパフォーマンスカウンタ「`Cisco Presence Engine`」の `ActiveJsmSessions` を監視するには、Cisco Real-Time Monitoring Tool（RTMT）を使用する必要があります。

- パブリッシャまたはサブスクライバを再起動した後
- Cisco XCP Router を再起動した後
- Cisco Presence Engine を再起動した後

高可用性を有効にする前に、「`Cisco Presence Engine`」の `ActiveJsmSessions` の数が、ノードに割り当てられたユーザの数と同じである必要があることを確認してください。

（注） ユーザの `ActiveJsmSessions` 作成の進行が完了した後にのみ、高可用性を有効にする必要があります。

手順

Step 1 Cisco Unified CM Administration のユーザ インターフェイスから、**[システム（System）] > [プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。

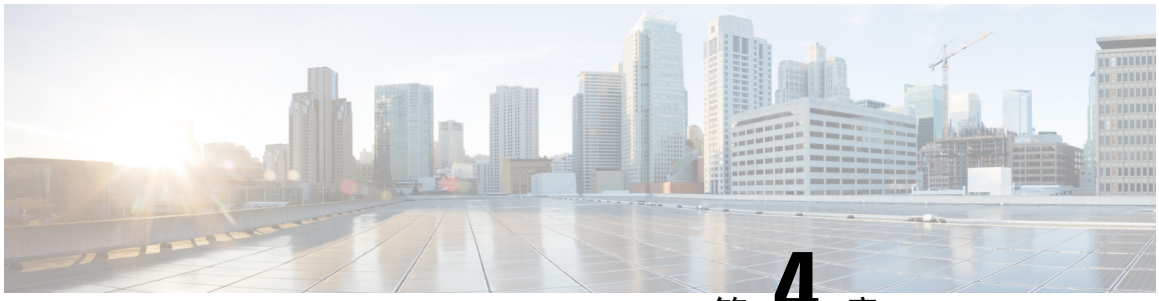
Step 2 **検索**をクリックして、グループを選択します。

プレゼンス冗長グループの設定 ウィンドウが表示されます。

Step 3 **ハイ アベイラビリティの有効化**のチェックボックスをチェックします。

Step 4 **[保存（Save）]** をクリックします。

Step 5 この手順を、各プレゼンス冗長グループに対して繰り返します。



第 4 章

IPv6 を設定する

IPv6 設定の概要

IM and Presence Service と Cisco Unified Communications Manager 間の接続に IPv4 を使用していても、IM and Presence Service では外部とのやりとりに IPv6 を使用できます。

IM and Presence Service ノードで次のいずれかの項目に IPv6 を設定する場合、ノードは着信する IPv4 パケットを受け入れず、自動的に IPv4 の使用に復帰することはありません。

- 外部データベースへの接続
- LDAP サーバへの接続
- Exchange サーバへの接続
- 連携の展開

フェデレーションでは、IPv6 が有効な外国企業へのフェデレーション リンクをサポートする必要がある場合は、IM and Presence Service で IPv6 を有効にする必要があります。これは、IM and Presence Service ノードとフェデレーション企業間に ASA がインストールされている場合にも当てはまります。ASA は、IM and Presence Service ノードに対して透過的です。

コマンドライン インターフェイスを使用して IPv6 パラメータを設定する場合の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*Cisco Unified Communications Manager* アドミニストレーション ガイド』および『*Cisco Unified Communications Solutions* コマンドライン インターフェイス ガイド』を参照してください。

IPv6 の設定タスクフロー

手順

	コマンドまたはアクション	目的
Step 1	IM and Presence Service 用 Eth0 を IPv6 で有効にする （40 ページ）	クラスタ内の各 IM and Presence Service ノードの Eth0 ポートで IPv6 を有効にします。各変更を適用するには、ノードを再起動する必要があります。
Step 2	IPv6 エンタープライズパラメータを有効にする （41 ページ）	Eth0 ポートで IPv6 を有効にした後、IM and Presence Service クラスタの IPv6 エンタープライズパラメータを有効にします。
Step 3	サービスを再起動する （41 ページ）	変更を適用するには、IM and Presence のサービスを再起動しなければなりません。
Step 4	IPv6 アドレスを IM and Presence Service ノードに割り当てる （42 ページ）	IPv6 アドレスを IM and Presence Service ノードに割り当てる

IM and Presence Service 用 Eth0 を IPv6 で有効にする

クラスタの各 IM and Presence Service ノードの Eth0 ポートで IPv6 を有効にするには、Cisco Unified IM and Presence Operating System の管理 GUI を使用します。

手順

Step 1 **Cisco Unified IM and Presence OS 管理**で、**設定** > **IP** > **イーサネット IPv6**を選択します。

Step 2 [イーサネット IPv6 設定] ウィンドウで、**ipv6の有効化** のチェックボックスをオンにします。

Step 3 **[アドレス ソース（Address Source）]** を選択します。

- ルータ アドバタイズメント
- DHCP
- 手動入力

手動入力を選択した場合は、**IPv6 アドレス**、**サブネット マスク**、および**デフォルト ゲートウェイ** の値を入力します。

Step 4 **[Update with Reboot（リブートを使用した更新）]** チェック ボックスをオンにします。

ヒント　予定されていたメンテナンス時間中などに、後で手動でノードを再起動する場合は、[リブートを使用した更新（Update with Reboot）] チェックボックスはオンにしないでください。ただし、変更した内容はノードがリブートされるまで有効になりません。

Step 5 [保存（Save）] をクリックします。

[リブートを使用した更新（Update with Reboot）] チェックボックスをオンにした場合は、ノードがリブートされ、変更が適用されます。

次のタスク

IPv6 エンタープライズパラメータを有効にする （41 ページ）

IPv6 エンタープライズパラメータを有効にする

IM and Presence Service クラスタの IPv6 エンタープライズ パラメータを有効にするには [Cisco Unified CM IM and Presence Administration（Cisco Unified CM IM and Presence の管理）] を使用します。

始める前に

IM and Presence Service 用 Eth0 を IPv6 で有効にする （40 ページ）

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**システム** > **エンタープライズ パラメータ**を選択します。

Step 2 **エンタープライズ パラメータの設定** ウィンドウで、IPv6 パネルの **有効** を選択します。

Step 3 **[保存（Save）]** をクリックします。

次のタスク

変更を適用するには、「サービスを再起動する （41 ページ）」 に移動します。

サービスを再起動する

クラスタの IPv6 エンタープライズ パラメータを有効にした後に、この手順で、IM and Presence サービスを再起動します。

ヒント [Cisco Unified CM IM and Presence Administration（Cisco Unified CM IM and Presence の管理）] を使用してシステム再起動通知をモニタするには、**[System（システム）]** > **[Notifications（通知）]** を選択します。

始める前に

IPv6 エンタープライズパラメータを有効にする （41 ページ）

手順

Step 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-ネットワークサービス（Control Center - Network Services）]** を選択します。

Step 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。

Step 3 **IM and Presence Services** エリアで、**Cisco XCP Router**を選択します。

Step 4 [再起動（Restart）] をクリックします。

Step 5 [関連リンク（Related Links）] ドロップダウン リストから [サービスのアクティブ化（Service Activation）] を選択し、[移動（Go）] をクリックします。

Step 6 **IM and Presence Services** のエリアで、以下のサービスを選択します。

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

Step 7 [保存（Save）] をクリックします。

IPv6 アドレスを IM and Presence Service ノードに割り当てる

この手順で、Cisco Unified Communications Manager で IM and Presence ノードの IPv6 アドレスを割り当てることができます。

始める前に

また、Cisco Unified OS の管理で IPv6 Eth0 ポートを有効にし、IPv6 エンタープライズ パラメータを有効にする必要もあります。

手順

Step 1 Cisco Unified Communications Manager のパブリッシャ ノードにログインします

Step 2 Cisco Unified CM の管理から、**[システム（System）]** > **[サーバ（Server）]** を選択します。

Step 3 次のいずれかのタスクを完了します。

- サーバを追加するには、**新規追加**をクリックします。
- 既存のサーバを更新するには、編集するサーバをクリックします。

Step 4 新しいサーバを追加する場合は、**サーバの種類**のドロップダウンメニューで、**CUCM IM and Presence** を選択して、**次へ** をクリックします。

Step 5 サーバの **IPv6 アドレス** を入力します。

Step 6 **[保存（Save）]** をクリックします。

Step 7 各 IM and Presence Service ノードでこれを繰り返します。

IM and Presence Service 用 Eth0 で IPv6 を無効にする

IPv6 を無効にするには、**Cisco Unified IM and Presence Operating System の管理** GUI を使用して、IPv6 を使用しないクラスタで各 IM and Presence サービス ノードの Eth0 ポートの IPv6 を無効にします。変更を適用するには、ノードを再起動する必要があります。

（注） IPv6 を使用するクラスタのいずれのノードも使用しない場合は、IPv6 エンタープライズ パラメータがクラスタで無効になっていることを確認します。

手順

Step 1 **Cisco Unified CM IM and Presence OS 管理**で、**設定** > **IP** > **イーサネット IPv6**を選択します。

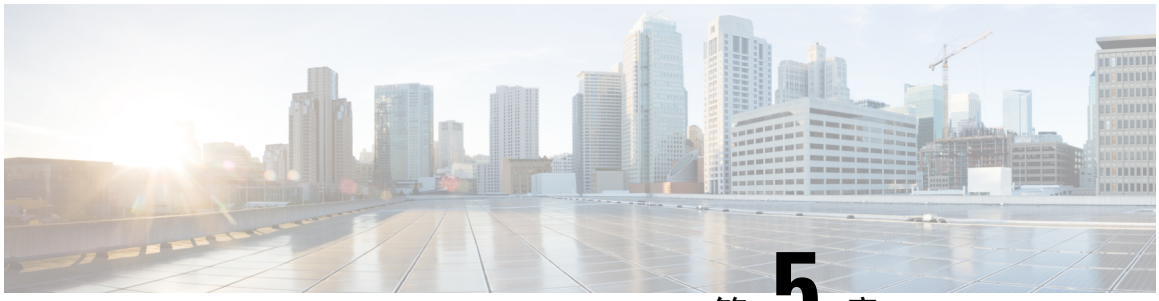
Step 2 [イーサネット IPv6 設定] ウィンドウで、**ipv6の無効化** のチェックボックスをオンにします。

Step 3 **[Update with Reboot（リブートを使用した更新）]** チェック ボックスをオンにします。

ヒント 予定されていたメンテナンス時間中などに、後で手動でノードを再起動する場合は、[リブートを使用した更新（Update with Reboot）] チェックボックスはオンにしないでください。ただし、変更した内容はノードがリブートされるまで有効になりません。

Step 4 [保存（Save）] をクリックします。

[リブートを使用した更新（Update with Reboot）] チェックボックスをオンにした場合は、ノードがリブートされ、変更が適用されます。



第 5 章

IM アドレススキームを設定する

IM アドレス スキーム：

IM and Presence Service は、次の 2 種類の IM アドレス指定スキームをサポートしています。

- *UserID@Default_Domain*が、IM and Presence Service をインストールした場合の、デフォルトの IM アドレス スキームです。
- Directory URI IM アドレス スキームは、複数のドメイン、ユーザのメール アドレスの調整、および Microsoft SIP URI の調整をサポートしています。

すべての IM and Presence Service クラスタ全体で、同じIM アドレス スキームを使用する必要があります。

User@Default_Domain を使用した IM アドレス

*UserID@Default_Domain*が、IM and Presence Service をインストールした場合の、デフォルトの IM アドレス スキームです。

UserID @ Default_Domain の IM アドレス スキームを使用すると、すべての IM アドレスが単一のデフォルト IM ドメインの一部となります。デフォルト ドメイン値は、すべてのクラスタ全体で一貫している必要があります。IM アドレスは IM and Presence のデフォルト ドメイン の一部であるため、複数ドメインはサポートされません。

UserID は、フリー フォームまたは LDAP から同期することができます。次のフィールドがサポートされます。

- sAMAccountName
- ユーザ プリンシパル名（UPN）
- 電子メール アドレス

- 従業員番号
- 電話番号

UserID を Cisco Unified Communications Managerの LDAP フィールドにマップする場合、その LDAP マッピングはすべてのクラスタ全体で一貫している必要があります。

ユーザ ID は電子メール アドレスにマッピング可能ですが、それが IM URI が電子メール アドレスと同じであるという意味ではありません。代わりに*<email-address>@Default_Domain*となります。たとえば、`amckenzie@example.com @sales-example.com` です。選択した設定をマッピングする Active Directory（AD）は、IM and Presence サービス クラスタ内のすべてのユーザに対してグローバルに適用されます。個々のユーザに対して異なるマッピングを設定することはできません。

ディレクトリ URI を使用した IM アドレス

ディレクトリ URI のアドレス スキームを使用して、ユーザの IM アドレスを Cisco Unified Communications Manager のディレクトリ URI に合わせます。

ディレクトリ URI の IM アドレス スキームには、次の IM アドレス指定機能があります。

- 複数ドメインのサポート。IM アドレスは、1 つの IM and Presence Service ドメインだけを使用する必要はありません。
- ユーザのメール アドレスの調整。ユーザのメール アドレスと合わせるように Cisco Unified Communications Manager のディレクトリ URI を設定することで、メール、IM、音声、および動画の通信にユーザの ID を一貫して指定できるようになります。
- Microsoft SIP URI の調整。Microsoft SIP URI と合わせるように Cisco Unified Communications Manager のディレクトリ URI を設定することで、Microsoft OCS/Lync から IM and Presence Service への移行時に、ユーザの ID を確実に維持できるようになります。

IM アドレス スキームとしてディレクトリ URI を使用するようにノードを設定する場合は、ディレクトリ URI をサポートするクライアントのみを展開することを推奨します。ディレクトリ URI をサポートしないクライアントは、ディレクトリ URI IM アドレス スキームが有効になっている場合は動作しません。ディレクトリ URI をサポートしないクライアントが展開されている場合は、*UserID@Default_Domain* IM アドレス スキームを使用し、ディレクトリ URI IM アドレス スキームは使用しないでください。

ディレクトリ URI IM アドレス設定はグローバルであり、クラスタ内のすべてのユーザに適用されます。クラスタ内の個々のユーザに対して異なるディレクトリ URI IM アドレスを設定できません。

外部 LDAP ディレクトリからのディレクトリ URI のプロビジョニングの詳細については、「LDAP ディレクトリの設定（85 ページ）」を参照してください。

複数の IM ドメイン

IM and Presence Service は、複数の IM アドレス ドメイン全体で IM アドレッシングをサポートし、システム内のすべてのドメインを自動的にリストします。ドメインの追加、編集、または削除を

行うことができます。IM ドメインの設定の詳細は、「ドメイン設定の概要 （25 ページ）」を参照してください。

Cisco Expressway を相互運用している場合は、http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.htmlの *Cisco Expressway* 管理ガイド を参照してください。

IM アドレス スキーム：

IM and Presence Service のデフォルト ドメインと、使用する IM アドレス スキームは、IM and Presence Service クラスタ全体で一貫している必要があります。はじめに、「IM and Presence Service のデフォルトドメインを設定する （32 ページ）」に進みます。

設定する IM アドレス スキームはすべてのユーザ JID に影響を与え、別の設定を持つ可能性があるクラスタ間での通信を中断せずに段階的に実行することはできません。

展開した クライアントが IM アドレスとしてディレクトリ URI をサポートしない場合は、管理者がディレクトリ URI IM アドレス スキームを無効にする必要があります。

IM アドレス スキームの設定のタスクフロー

IM アドレス スキームを設定するには、以下の順序でこのタスクを完了してください。

手順

	コマンドまたはアクション	目的
Step 1	ユーザープロビジョニングを確認する （48 ページ）	エンド ユーザが適切にプロビジョニングされていること、および重複しているユーザまたは無効なユーザがいないことを確認します。
Step 2	高可用性を無効にする （49 ページ）	プレゼンス冗長グループのハイ アベイラビリティは、一時的に無効にする必要があります。IM アドレス スキームを設定するには、一時的にサービスを停止する必要があります。ハイ アベイラビリティが有効のままサービスを停止すると、システム フェールオーバーが発生します。
Step 3	サービスを停止する （50 ページ）	IM アドレッシングスキームの設定を更新する前に、不可欠な IM and Presence サービスを停止します。指定された順序でサービスを停止することを確認します。

	コマンドまたはアクション	目的
Step 4	IMアドレス スキームの割り当て（50ページ）	この手順を使用して、新しいドメインとIM アドレススキームを設定するか、既存のドメインとアドレススキームを更新します。
Step 5	サービスを再起動する （52 ページ）	IM アドレッシングスキームが設定されたら、サービスを再起動します。これは、ユーザ アドレス情報を更新したり新しいユーザをプロビジョニングしたりする前に実行する必要があります。サービスの起動は、必ず所定の順序で行ってください。
Step 6	高可用性の有効化 （53 ページ）	IM アドレス スキームを設定し、IM and Presence サービスを再起動した後で、プレゼンス冗長グループのハイ アベイラビリティを有効にすることができます。ハイ アベイラビリティを有効化する前に、すべてのサービスが IM and Presence データベース パブリッシャ ノードおよびサブスクライバ ノードで稼働していなければなりません。
Step 7	IMアドレス スキームとして**ディレクトリ URI** を選択した場合： • ディレクトリ URI への LDAP ソースの割り当て （54 ページ） • ディレクトリ URI の手動割り当て （55 ページ）	オプション。外部 LDAP ディレクトリからユーザを同期している場合は、ディレクトリの URI 値の [LDAP ソース] フィールドを設定します。 LDAP 以外のユーザの場合は、ディレクトリ URI を手動でプロビジョニングする必要があります。これは、ユーザ単位で行うか、一括管理ツールを使用して行うことができます。

ユーザープロビジョニングを確認する

アドレス スキームを設定する前に、この手順を使用して、エンドユーザが適切にプロビジョニングされていることを確認してください。

手順

Step 1 Cisco Unified CM IM and Presence Administration から、 **診断** > **システムのトラブルシューティング** を選択します。
システムのトラブルシューティングが実行されます。

Step 2 **ユーザのトラブルシューティング**のセクションで、エンドユーザが適切にプロビジョニングされていること、また、重複しているユーザまたは無効なユーザがいないことを確認します。

次のタスク

高可用性を無効にする （49 ページ）

高可用性を無効にする

各プレゼンス冗長グループに対するハイアベイラビリティを無効にします。アドレススキームを編集するには、サービスを一時的に停止する必要があります。ハイ アベイラビリティが有効になったサービスを停止すると、システム フェールオーバーが発生します。

（注） [**プレゼンス冗長グループの詳細**]ページには、クラスタで高可用性が無効になっている場合でも、すべてのアクティブな JSM セッションが表示されます。

始める前に

各プレゼンス冗長グループの各クラスタ ノードのアクティブ ユーザ数を記録します。この情報は、Cisco Unified CM IM and Presence の（**System** > **Presence Topology**）ウィンドウに表示されます。この番号は、後にハイ アベイラビリティを再度有効にする際に必要となります。

手順

Step 1 Cisco Unified CM Administration のユーザ インターフェイスから、**[システム（System）] > [プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。

Step 2 **検索**をクリックして、グループを選択します。

Step 3 [プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウで、**[ハイ アベイラビリティを有効にする（Enable High Availability）]** チェックボックスをオフにします。

Step 4 [保存（Save）] をクリックします。

Step 5 各プレゼンス冗長グループに対して、この手順を繰り返します。

Step 6 完了後、さらに変更を行う前に、新しい HA 設定がクラスタ全体にわたって同期されるまで、少なくとも 2 分待機します。

次のタスク

サービスを停止する （50 ページ）

サービスを停止する

IMアドレッシングスキームの設定を更新する前に、不可欠なIM and Presenceサービスを停止します。指定された順序でサービスを停止することを確認します。

始める前に

高可用性を無効にする （49 ページ）

手順

Step 1 **Cisco Unified IM and Presence サービスアビリティ**で、**ツール** > **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。

Step 2 サービスを選択し、[**停止 (Stop)**] ボタンをクリックして、次の IM and Presence サービスをこの順序で停止します。

a) **Cisco Sync Agent**
b) **Cisco Client Profile Agent**

Step 3 両方のサービスが停止したら、[Tools] [> **Control Center-Feature services**] を選択し、次のサービスをこの順序で停止します。

a) **Cisco Presence Engine**
b) **Cisco SIP Proxy**

Step 4 両方のサービスが停止したら、[Tools] [> **Control Center-Feature services**] を選択し、次のサービスを停止します。

- **Cisco XCP Router**

（注） XCPルータサービスを停止すると、関連するすべてのXCP機能サービスが自動的に停止します。

次のタスク

IM アドレス スキームの割り当て （50 ページ）

IM アドレス スキームの割り当て

この手順を使用して、新しいドメインと IM アドレススキームを設定するか、既存のドメインとアドレススキームを更新します。

（注） 設定する IM アドレス スキームは、必ずすべてのクラスタ間で一致するようにしてください。

始める前に

サービスを停止する （50 ページ）

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**プレゼンス** > **設定** > **詳細設定**を選択します。

Step 2 新しいデフォルトドメインを割り当てるには、[**Default domain**] チェックボックスをオンにし、テキストボックスに新しいドメインを入力します。

Step 3 アドレススキームを変更するには、[**IM アドレススキーム (IM Address scheme**)] チェックボックスをオンにして、ドロップダウンリストボックスから次のいずれかのオプションを選択します。

- **UserID@[Default_Domain] —:** 各 IM ユーザ アドレスは、UserID からデフォルト ドメインと共に取得されます。これがデフォルト設定です。
- **ディレクトリ URI —:** 各 IM ユーザ アドレスは、Cisco Unified Communications Manager でそのユーザに関して設定されているディレクトリ URI と一致します。

  （注） このオプションを選択すると、展開されたすべてのクライアントが、IMアドレスとしてディレクトリ URI をサポートし、EDI ベースまたは UDS ベースのディレクトリ統合に対応している必要があります。Jabber との UDS ベースの統合を行うには、Jabber のリリース 10.6 以降を実行している必要があります。

Step 4 [保存（Save）] をクリックします。

ステータス領域の更新進行状況を監視できます。

IM アドレス スキームとしてディレクトリ URI を選択する場合、展開クライアントが複数ドメインをサポートできることを確認するプロンプトが表示される場合があります。続行するには **[OK（OK）]** をクリックします。または **[取消（Cancel）]** をクリックします。

ユーザが [ディレクトリ URI（Directory URI）] 設定を無効にしている場合は、ダイアログボックスが表示されます。続行するには、**[OK（OK）]** をクリックし、または **[取消（Cancel）]** をクリックします。次に、IM アドレス スキームを再設定する前にユーザ設定をします。

システム アップデートは完了まで最長で 1 時間かかる場合があります。変更を再適用するには、**[再試行（Re-try）]** をクリックします。または **[取消（Cancel）]** をクリックします。

次のタスク

アドレス指定スキームとして user @ default_domain を設定し、ディレクトリ URI を使用していない場合は、サービスを再起動する （52 ページ）に進みます。

アドレス スキームとしてディレクトリ URI を設定した場合は、以下のオプションのいずれかを選択します。

- ディレクトリ URI への LDAP ソースの割り当て （54 ページ）

- ディレクトリ URI の手動割り当て（55 ページ）

IM アドレスの例

IM and Presence Service で使用可能な IM アドレス オプションの例。

IM and Presence Service デフォルト ドメイン：cisco.com
ユーザ：：山田太郎
ユーザ ID： ty12345
メール ID： tyamada@cisco-sales.com
SIPURI：：taro.yamada@webex.com

IM アドレス形式	ディレクトリ URI マッピング	IM アドレス
<userid>@<domain>	該当なし	js12345@cisco.com
[ディレクトリ URI（Directory URI）]	mailid	jsmith@cisco-sales.com
[ディレクトリ URI（Directory URI）]	msRTCSIP-PrimaryUserAddress	john.smith@webex.com

サービスを再起動する

IM アドレッシングスキームが設定されたら、サービスを再起動します。これは、ユーザ アドレス情報を更新したり新しいユーザをプロビジョニングしたりする前に実行する必要があります。サービスの起動は、必ず所定の順序で行ってください。

始める前に

- IM アドレス スキームの割り当て（50 ページ）
- アドレス スキームとしてディレクトリ URI を設定した場合は、サービスを再起動する前に以下のオプションのいずれかを完遂します。
  - ディレクトリ URI への LDAP ソースの割り当て（54 ページ）
  - ディレクトリ URI の手動割り当て（55 ページ）

手順

Step 1 **Cisco Unified IM and Presence サービスアビリティ**で、**ツール > 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。

Step 2 サービスを選択し、[起動（Start）] ボタンをクリックして、次のサービスを起動します。

- **Cisco XCP Router**

Step 3 サービスが起動したら、[Tools] [> **Control Center-Feature Services**] を選択し、次のサービスをこの順序で開始します。

a) **Cisco SIP Proxy**
b) **Cisco Presence Engine**

Step 4 次の手順に進む前に、Cisco Presence Engine サービスがすべてのノードで実行されていることを確認します。

Step 5 **[Tools]** > **[Control Center – Network Services]** を選択し、次のサービスをこの順序で開始します。

a) **Cisco Client Profile Agent**
b) **Cisco Sync Agent**

次のタスク

高可用性の有効化 （53 ページ）

高可用性の有効化

IM アドレス スキームを設定し、サービスを再起動した後に、クラスタ内の各プレゼンス冗長グループのハイ アベイラビリティを再度有効にするには、以下の手順に従います。

始める前に

ハイ アベイラビリティを有効化する前に、すべてのサービスが IM and Presence データベース パブリッシャ ノードおよびサブスクライバ ノードで稼働していなければなりません。サービスが再起動してから30分以内の場合は、ハイ アベイラビリティを有効にする前に Cisco Jabber セッションが再作成されたことを確認します。十分な時間を確保しない場合、セッションが作成されていない Jabber クライアントでプレゼンスは機能しません。

Cisco Jabber セッションの数を取得するには、すべてのクラスタ ノードで `show perf query counter Cisco Presence Engine Active JsmSessions` CLI コマンドを実行します。アクティブ セッションの数は、ハイ アベイラビリティを無効にした際に記録したユーザ数と一致するはずです。

手順

Step 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-ネットワークサービス（Control Center - Network Services）]** を選択します。

Step 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。

Step 3 **IM and Presence Services** のエリアで、以下のサービスを選択します。

- **Cisco Client Profile Agent**
- **Cisco Sync Agent**
- **Cisco XCP Router**

Step 4 [再起動（Restart）] をクリックします。

Step 5 [関連リンク（Related Links）] ドロップダウン リストから [サービスのアクティブ化（Service Activation）] を選択し、[移動（Go）] をクリックします。

Step 6 **IM and Presence Services** のエリアで、以下のサービスを選択します。

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

Step 7 [保存（Save）] をクリックします。

ディレクトリ URI への LDAP ソースの割り当て

外部 LDAP ディレクトリからユーザを同期している場合は、この手順を使用して、ディレクトリ URI を割り当てに使用する外部 LDAP ディレクトリのソース フィールドを割り当てることができます。LDAP ディレクトリの同期が行われると、設定したフィールドの値からディレクトリ URI が割り当てられます。

（注） 最初の LDAP 同期がすでに行われていた場合、Cisco Unified Communications Manager では、LDAP ディレクトリの既存の設定に新しい設定を追加することはできません。外部 LDAP ディレクトリに追加された新しいアイテムを同期することはできても、Cisco Unified Communications Manager で LDAP 設定を編集することはできません。すでに LDAP ディレクトリを同期していた場合：

- ディレクトリ URI をユーザに割り当てるには、バルク管理ツールを使用します。詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。
- ユーザにディレクトリ URI を手動で割り当てます。

始める前に

IM アドレス スキームの割り当て （50 ページ）

手順

Step 1 Cisco Unified CM 管理から、**システム** > **LDAP** > **LDAP ディレクトリ**を選択します。

Step 2 **ディレクトリ URI**のドロップダウン リストから、次のいずれかのオプションを選択します。

- **メール：**ユーザのメールアドレスと合わせてディレクトリ URI を設定することで、メール、IM、音声、および動画の通信にユーザの ID を一貫して指定できるようになります。
- **msRTCSIP-PrimaryUserAddress：**ディレクトリ URI を Microsoft OCS/Lync SIP URI（msRTCSIP-PrimaryUserAddress）にマップします。

（注） ディレクトリ URI は、LDAP 同期が行われるまでプロビジョニングされません。LDAP ディレクトリ同期の設定の詳細は、「LDAP ディレクトリの設定（85 ページ）」を参照してください。

次のタスク

サービスを再起動する（52 ページ）

ディレクトリ URI の手動割り当て

LDAP を使用していない場合は、この手順を使用して、ユーザ毎にディレクトリ URI を手動で入力することができます。

（注） また、一括管理ツールを使用して、CSVファイル経由で、ディレクトリ URI を多数のエンドユーザにプロビジョニングすることもできます。一括管理の使用方法の詳細は、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html の *Cisco Unified Communications Manager* 一括管理ガイドを参照してください。

LDAP ディレクトリが未同期の場合は、LDAP ディレクトリ同期を使用してユーザのディレクトリ URI をプロビジョニングすることができます。

始める前に

IM アドレス スキームの割り当て（50 ページ）

手順

Step 1 **Cisco Unified CM 管理**で、**ユーザ管理** > **エンド ユーザ**を選択します。

Step 2 適切な検索条件を入力し、[検索（Find）] をクリックします。

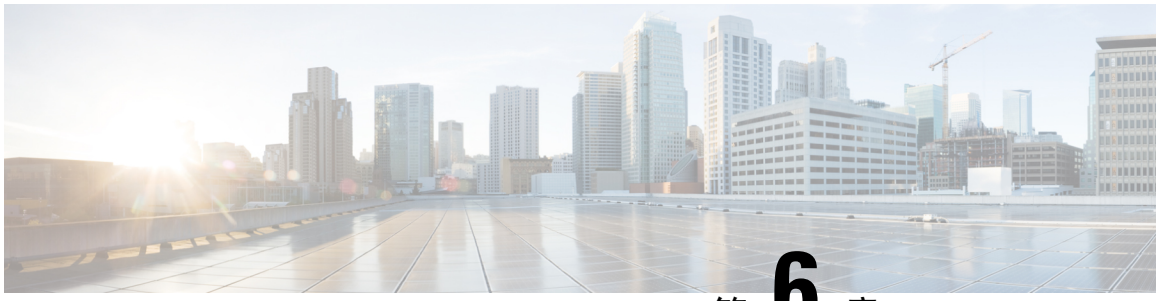
Step 3 設定するエンド ユーザを選択します。

Step 4 **ユーザ情報** エリアで、**ディレクトリ URI** フィールドにディレクトリ URI を入力します。

Step 5 [保存（Save）] をクリックします。

次のタスク

サービスを再起動する （52 ページ）



第 6 章

冗長性およびハイ アベイラビリティの設定

プレゼンス冗長グループの概要

プレゼンス冗長グループは、同じクラスタからの 2 つの IM and Presence Service ノードで設定されています。プレゼンス冗長グループ内の各ノードは、ピア ノードのステータスまたはハートビートをモニタします。プレゼンス冗長グループを設定して、IM and Presence サービスのクライアントとアプリケーションの両方の冗長性と回復を提供することができます。

- フェールオーバー：プレゼンス冗長グループ内の IM and Presence サービス ノード上で 1 つ以上の重要なサービスが失敗した場合、またはグループ内のノードが失敗した場合、プレゼンス冗長グループ内で行われます。クライアントは、そのグループ内のもう 1 つの IM and Presence サービス ノードに自動的に接続します。
- フォールバック：以下のいずれかの状況で、フォールバック コマンドが CLI またはCisco Unified Communications Manager から発行されると行われます。
  - 失敗した IM and Presence サービス ノードがサービスを再開し、すべての重要なサービスが動作している場合。サービスが再開されると、グループ内のフェールオーバーしていたクライアントは回復したノードに再接続されます。
  - 重要なサービスの不具合のために、アクティブ化されていたバックアップ IM and Presence サービス ノードが失敗し、ピア ノードがフェールオーバー状態であり、自動回復フォールバックをサポートしている場合。

たとえば、ローカルの IM and Presence サービスノードのサービスまたはハードウェアで障害が発生した場合、Cisco Jabber クライアントは、プレゼンス冗長グループを使用してバックアップ用 IMとプレゼンスサービス ノードにフェールオーバーします。障害が発生したノードが再びオンラ

インになると、自動フォールバックを構成すると、クライアントは自動的にローカルのIM and Presence サービスノードに再接続されます。自動フォールバックを設定していない場合は、失敗したノードがオンラインになったときに、手動でフォールバックを開始できます。

プレゼンス冗長性グループでは、冗長性と回復だけでなく、クラスタの高可用性を設定することもできます。

高可用性

IMとプレセンスサービスは、マルチノード導入の高可用性をサポートしています。

プレゼンス冗長グループを設定した後は、そのグループの高可用性を有効にすることができます。高可用性を実現するには、ペアのノードが必要です。各ノードには、独立型のデータベースと一連のユーザが存在し、これらは、共通のユーザをサポートできる共有アベイラビリティ データベースとともに運用されます。

すべてのIM and Presence サービスノードが、プレゼンス冗長グループに属している必要があります。このグループは、単一の IM and Presence サービスノード、またはペアのIM and Presence サービスノードで構成されている場合があります。

高可用性を設定するには、次の 2 つの異なるモードを使用します。

- バランスモード:このモードでは、自動ユーザロードバランシング機能と、コンポーネントの障害や停電が原因で障害が発生した場合のユーザフェイルオーバー機能を備えた、冗長高可用性を提供します。
- プライマリスペアモード:プライマリノードに障害が発生した場合、スタンバイノードは自動的にプライマリノードを引き継ぎます。自動ロードバランシング機能は提供しません。

IM and Presence サービの導入を高可用性の導入として設定することをお勧めします。シングル導入で高可用性と非高可用性状態の冗長グループを同時に構成することは可能ですが、この構成は推奨されません。

プレゼンス冗長グループの要件

WANを使用した配置の場合、各IM and Presence サービス クラスタに対して最低 10 メガビット/秒の専用帯域幅と、80ミリ秒以下のラウンドトリップ遅延が必要です。この推奨帯域幅よりも小さい帯域幅では、パフォーマンスに悪い影響を及ぼす可能性があります。

プレゼンス冗長グループのタスク フロー

1 つの IM and Presence Service ノードは、1 つのプレゼンス冗長グループのみに割り当てることができます。高可用性を実現するには、同じクラスタから 2 つのノードをプレゼンス冗長グループに割り当て、グループの高可用性を確保する必要があります。

手順

	コマンドまたはアクション	目的
Step 1	データベースのレプリケーションの確認（59 ページ）	データベース レプリケーションが IM and Presence サービス クラスタで設定されていることを確認します。
Step 2	サービスの確認 （60 ページ）	重要なサービスがプレゼンス冗長グループに追加予定のノード上で実行されていることを確認します。
Step 3	プレゼンス冗長グループの設定 （61 ページ）	IM and Presence Service クライアントとアプリケーションの冗長性とリカバリを提供します。
Step 4	フェール オーバーのハートビート間隔の設定 （62 ページ）	（省略可）プレゼンス冗長グループ内の各ノードは、ピア ノードのステータスまたはハートビートをモニタします。各ノードがピアをモニタする間隔を設定できます。
Step 5	高可用性の有効化 （63 ページ）	（省略可）プレゼンス冗長グループを設定したときに高可用性を有効にしなかった場合は、この手順を実行します。
Step 6	ユーザ割り当てモードの設定 （64 ページ）	Sync Agent が IM and Presence サービス クラスタのさまざまなノード全体にユーザを分散する方法を設定します。この設定は、システムがフェールオーバーと負荷分散を処理する方法に影響します。

データベースのレプリケーションの確認

状態冗長グループの高可用性を有効にする前に、IM and Presence サービスクラスタでデータベースレプリケーションが設定されていることを確認してください。

手順

Step 1 次のいずれかの方法を使用して CLI セッションを開始します。

- リモート システムの場合は、SSH を使用して Cisco Unified オペレーティング システムにセキュアに接続します。SSH クライアントで、**ssh *adminname* @ *hostname***を入力してパスワードを入力します。
- シリアル ポートへの直接接続を介して、自動的に表示されるプロンプトでクレデンシャルを入力します。

Step 2 **utils dbreplication status** コマンドを実行して、データベース テーブルのエラーまたは不一致を確認します。

Step 3 **utils dbreplication runtimestate** コマンドを実行して、ノードでデータベース レプリケーションがアクティブであることを確認します。

出力にはすべてのノードが一覧表示されます。データベース レプリケーションがセットアップされて正常であれば、各ノードの **replication setup** の値は **2** になります。

2 以外の値が返された場合は、続行する前にエラーを解決する必要があります。

次のタスク

サービスの確認 （60 ページ）

サービスの確認

重要なサービスがプレゼンス冗長グループに追加予定のノード上で実行されていることを確認します。高可用性を有効にする前に、重要なサービスを実行する必要があります。重要なサービスがいずれのノードでも動作していない場合、障害状態に高可用性をオンにするとプレゼンス冗長グループは Failed 状態になります。重要なサービスが 1 つのノードで実行されていない場合、高可用性をオンにすると、そのノードが他のノードにフェールオーバーします。

始める前に

データベースのレプリケーションの確認 （59 ページ）

手順

Step 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。

Step 2 [サーバ（Server）] リストから、適切なノードを選択し、[移動（Go）] をクリックします。

Step 3 [IM and Presence サービス（IM and Presence Services）] で、次のサービスが開始されていることを確認します。

- **Cisco Client Profile Agent**
- **Cisco Sync Agent**
- **Cisco XCP Router**

Step 4 [関連リンク（Related Links）] ドロップダウン リストから [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、[移動（Go）] をクリックします。

Step 5 [IM and Presence サービス（IM and Presence Services）] で、次のサービスが開始されていることを確認します。

- **Cisco SIP Proxy**
- **Cisco Presence Engine**

次のタスク

プレゼンス冗長グループの設定 （61 ページ）

プレゼンス冗長グループの設定

Cisco Unified Communications Managerを使用して、IM and Presence サービスノードの冗長性を構成します。

各状態冗長グループには、2つのIM and Presence サービスノードを含めることができます。各ノードは、1つのプレゼンス冗長グループにのみ割り当て可能です。プレゼンス冗長グループの両方のノードが同一クラスタ上にあり、同じ IM and Presence サービス データベース パブリッシャ ノードを持つ必要があります。

始める前に

- サービスの確認 （60 ページ）
- 状態冗長グループに追加するIM and Presence サービスノードが同じソフトウェアバージョンを実行していることを確認します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]>[プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。

Step 2 **[新規追加]** をクリックします。

Step 3 ステータスが冗長なグループの一意の名前を入力します。

アンダースコア（_）とダッシュ（-）を含む最大 128 字の英数字を入力できます。

Step 4 グループの説明を入力します。

記号を含む最大 128 字の英数字を入力できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、スラッシュ（\）、山カッコ（<>）は使用できません。

Step 5 IM and Presence Serviceの 2 つの異なるノードを [プレゼンス サーバ（Presence Server）] フィールドで選択し、グループに割り当てます。

Step 6 （任意） [高可用性を有効にする（Enable High Availability）] チェックボックスをオンにして、プレゼンス冗長グループの高可用性を有効にします。

Step 7 [保存（Save）] をクリックします。

次のタスク

フェール オーバーのハートビート間隔の設定 （62 ページ）

フェール オーバーのハートビート間隔の設定

プレゼンス冗長グループ内の各ピアが、ピアがアクティブであることを確認するためには、ピア ノードのハートビート（ステータス）をモニタするキープ アライブ設定を決定する任意指定のサービス パラメータを設定します。フェールオーバーは、設定したタイマーの有効期限が切れた後にピア ノードが応答しなくなった場合に開始されます。

（注） シスコでは、このパラメータのデフォルト値を使用することを推奨しています。ただし、必要に応じて値を設定し直すことも可能です。

手順

Step 1 Cisco Unified CM IM and Presence Administration で、**システム** > **サービス パラメータ**を選択します。

Step 2 [サーバ（Server）] ドロップダウン リストから、IM and Presence ノードを選択します。

Step 3 [サービス（Service）] ドロップダウンから、**Cisco Server Recovery Manager**（**アクティブ**）を選択します。

Step 4 [一般的なServer Recovery Managerパラメータ（クラスタ全体）（General Server Recovery Manager Parameters (Clusterwide)）] で、プレゼンス冗長グループ内の各ノードがピア ノードのハートビートのモニタに使用する、クラスタ全体のキープ アライブ設定を指定します。フェールオーバーは、ピア ノードが応答しない場合に開始することができます。

- **[サービスポート（Service Port）]**：このパラメータでは、Cisco Server Recovery Manager がピアとの通信に使用するポートを指定します。デフォルトは 22001 です。
- **[管理RPCポート（Admin RPC Port）]**：このパラメータでは、Cisco Server Recovery Manager が管理 RPC 要求を提供するために使用するポートを指定します。デフォルトは 20075 です。
- **[重要なサービス遅延（Critical Service Delay）]**：このパラメータでは、フェールオーバーが開始されるまでに重要なサービスを停止しても無視される期間を、秒単位で指定します。デフォルトは 90 です。
- **[自動フォールバックの有効化（Enable Automatic Fallback）]**：このパラメータでは、自動フォールバックを実行するかどうかを指定します。フェールオーバーが発生した場合、プライマリ ノードが正常な状態に戻った 30 分後に、IM and Presence Service がユーザをバックアップ ノードからプライマリ ノードに自動的に移動します。デフォルト値は [False] です。
- **[初期化キープアライブ（ハートビート）タイムアウト（Initialization Keep Alive (Heartbeat) Timeout）]**：このパラメータでは、フェールオーバーが開始されるまでに、初期化中にピア

との間でハートビートが喪失しても無視される期間を、秒単位で指定します。デフォルトは 120 です。

- **[キープアライブ（ハートビート）タイムアウト（Keep Alive (Heartbeat) Timeout）]**：このパラメータでは、フェールオーバーが開始されるまでに、ピアとの間でハートビートが喪失しても無視される期間を、秒単位で指定します。デフォルトは 60 です。
- **[キープアライブ（ハートビート）間隔（Keep Alive (HeartBeat) Interval）]**：このパラメータでは、ピア ノードに送信されるキープアライブ（ハートビート）メッセージの間隔を指定します。デフォルトは 15 です。
- **[XCP Authentication Serviceのモニタリングの有効化（Enable monitoring of XCP Authentication Service）]**：このパラメータを使用して、Cisco XCP Authentication Service をモニタするようにシステムを設定し、ノードでサービスの障害が発生したときにピア ノードへの自動フェールオーバーを開始することができます。[XCP Authentication Serviceのモニタリングの有効化（Enable monitoring of XCP Authentication Service）] フィールドで、サービス パラメータの値を [TRUE] に設定します。

Step 5 次の追加パラメータを設定して、CUPC 8.5 以降のクライアントに、再ログインを試行するまでの待機時間を指定します。前述のパラメータとは異なり、これらのパラメータは、クラスタ ノード毎に個別に設定する必要があります。

- **[クライアントの再ログインの下限（Client Re-Login Lower Limit）]**：このパラメータでは、CUPC 8.5 以降がこのサーバに再ログインするまでの待機時間の加減を秒単位で指定します。デフォルトは 120 です。
- **[クライアントの再ログインの上限（Client Re-Login Upper Limit）]**：このパラメータでは、CUPC 8.5 以降がこのサーバに再ログインするまでの待機時間の上限を秒単位で指定します。デフォルトは 537 です。

Step 6 **[保存（Save）]** をクリックします。

次のタスク

プレゼンス冗長グループを設定したときに「高可用性の有効化 （63 ページ）」を実行しなかった場合は、ここで実行します。

高可用性の有効化

注意 IM and Presence Service クラスタのレプリケーションのセットアップに失敗したが、すべての重要なサービスが実行されている場合、現在の冗長グループで有効な場合は、すぐにフェール オーバーする場合があります。

始める前に

- プレゼンス冗長グループの設定 （61 ページ）

- IM and Presence Service クラスタでレプリケーションがセットアップされていることを確認します。
- すべての重要なサービスが動作していることを確認します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。

Step 2 検索情報を指定し、[検索（Find）] をクリックします。

Step 3 設定したプレゼンス冗長グループを選択します。

Step 4 高可用性を有効にするには、[高可用性を有効にする（Enable High Availability）] チェックボックスをオンにします。

Step 5 [保存（Save）] をクリックします。

ユーザ割り当てモードの設定

この手順を使用して、同期エージェントがクラスタ内のノードにユーザーを割り当てる方法を構成します。この設定は、フェールオーバーと負荷分散を管理するのに役立ちます。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

Step 2 [ユーザ管理パラメータ（User Management Parameters）] 領域で、[プレゼンスサーバのユーザ割り当てモード（User Assignment Mode for Presence Server）] パラメータに次のいずれかのオプションを選択します。

- [バランス（Balanced）]：このモード（デフォルト）では、ユーザを各サブクラスタのそれぞれのノードに均等に割り当て、各ノードにユーザの合計数が均等に分散するようにします。これがデフォルトのオプションです。
- [アクティブスタンバイ（Active-Standby）]：このモードでは、サブクラスタの最初のノードにすべてのユーザを割り当て、セカンダリ サーバをバックアップのままにします。
- **[なし（None）]**：このモードでは、Sync Agent でクラスタのノードにユーザが割り当てられません。

Step 3 [保存（Save）] をクリックします。

手動フェールオーバー、フォールバック、リカバリの開始

この手順で、プレゼンス冗長グループの IM and Presence Service ノードのフェール オーバー、フォール バックおよびリカバリを手動で開始することができます。

- 手動フェールオーバー：手動フェールオーバーを開始すると、**Cisco Server Recovery Manager** が、障害が発生したノードの重要なサービスを停止します。失敗したノードのすべてのユーザの接続は切断され、再度バックアップ ノードにログインする必要があります。手動フォールバックを呼び出さない限り、重要なサービスは再起動されません。
- 手動フォールバック：手動フォールバックを開始すると、**CiscoServer Recovery Manager**がプライマリ ノード上の重要なサービスを再起動し、フェールオーバーが行われたすべてのユーザの接続を切断します。これらのユーザは、割り当てられたノードに再度ログインする必要があります。
- 手動リカバリ：プレゼンス冗長グループ内の両方のノードが障害状態となった場合、手動で回復する必要があります。この場合、IM and Presence Service が **Cisco Server Recovery Manager** サービスを、プレゼンス冗長グループの両方のノードで再起動します。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]**>**[プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。

Step 2 **検索**をクリックして、適切なノードを持つプレゼンス冗長グループを選択します。

Step 3 次のいずれかを実行します。使用可能なボタンは、ノードの現在の状態によって異なることに留意してください。

- **フェール オーバー**をクリックして、アクティブノードのフェール オーバーを開始します。
- **フォール バック** をクリックして、フェール オーバーされたノードのフォール バックを開始します。
- 両方のノードがフェイル オーバーして、リカバリを行う場合は、**リカバリ**をクリックします。

（注） これらの操作は、CLI を使用して、Cisco Unified Communications Manager または IM and Presence Service から開始することも可能です。詳細については、『*Cisco Unified Communications* ソリューション コマンドライン インターフェイス ガイド』を参照してください。

（注） いずれかのノードがフェール オーバー状態である間のエンド ユーザの IM and Presence Service クラスタへの追加はできません。

ノード状態の定義

表 *4:* プレゼンス冗長グループのノード状態の定義

状態	説明
初期化中（Initializing）	Cisco Server Recovery Manager サービスが開始した際の一時的な初期（遷移）状態です。
アイドル（Idle）	フェールオーバーが発生してサービスが停止すると、IM and Presence サービスはアイドル状態になります。アイドル状態では、IM and Presence Service ノードは可用性サービスやインスタント メッセージ サービスを提供しません。[Cisco Unified CMの管理（Cisco Unified CM Administration）] ユーザ インターフェイスを使用して、このノードへのフォールバックを手動で開始できます。
正常（Normal）	安定した状態です。IM and Presence Service が正常に稼働しています。この状態では、[Cisco Unified CMの管理（Cisco Unified CM Administration）] ユーザインターフェイスを使用して、このノードへのフェールオーバーを手動で開始できます。
バックアップ モードで実行中（Running in Backup Mode）	安定した状態です。IM and Presence サービス ノードは、ピア ノードのバックアップとして機能中です。ユーザはこの（バックアップ）ノードに移動されました。
テイク オーバー中（Taking Over）	遷移状態です。IM and Presence サービス ノードは、ピア ノードのテイクオーバー中です。
フェールオーバー中（Failing Over）	遷移状態です。IM and Presence サービス ノードは、ピア ノードによってテイクオーバーされています。
フェールオーバー済み（Failed Over）	安定した状態です。IM and Presence Service ノードがフェールオーバーしましたが、重要なサービスはダウンしていません。この状態では、[Cisco Unified CMの管理（Cisco Unified CM Administration）] ユーザ インターフェイスを使用して、このノードへのフォールバックを手動で開始できます。
フェールオーバー済み（重要なサービスは非実行）（Failed Over with Critical Services Not Running）	安定した状態です。IM and Presence Service ノード上の一部の重要なサービスが停止または失敗しました。

状態	説明
フォールバック中（Falling Back）	遷移状態です。システムは、バックアップ モードで実行中のノードから、この IM and Presence サービス ノードにフォールバック中です。
テイク バック中（Taking Back）	遷移状態です。障害が発生した IM and Presence Service ノードが、ピアから引き継ぎ直します。
障害モードで実行中（Running in Failed Mode）	遷移状態または[バックアップモードで実行中（Running in Backup Mode）]状態のときにエラーが発生しました。
不明（Unknown）	ノード状態は不明です。 考えられる原因は、IM and Presence Service ノードで高可用性が適切に有効化されていないことです。プレゼンス冗長グループの両方のノードで、Server Recovery Manager サービスを再起動します。

ノードの状態、原因、および推奨するアクション

[Cisco Unified CMの管理(Cisco Unified CM Administration)] ユーザ インターフェイスを使用してグループを選択する場合、[プレゼンス冗長グループの設定(Presence Redundancy Group Configuration)] ウィンドウのプレゼンス冗長グループでノードのステータスを表示できます。

表 *5:* プレゼンス冗長グループ ノードの高可用性状態、原因、および推奨されるアクション

ノード 1		ノード 2		
状態	理由	状態	理由	原因/推奨するアクション
正常（Normal）	正常（Normal）	正常（Normal）	正常（Normal）	正常（Normal）
フェールオーバー中（Failing Over）	管理者の要求による	テイクオーバー中（Taking Over）	管理者の要求による	管理者がノード 1 からノード 2 への手動フェールオーバーを開始しました。手動フェールオーバーの処理中です。
アイドル（Idle）	管理者の要求による	バックアップ モードで実行中（Running in Backup Mode）	管理者の要求による	管理者が開始したノード 1 からノード 2 への手動フェールオーバーが完了しました。

ノード1		ノード2		
状態	理由	状態	理由	原因/推奨するアクション
テイクバック中（Taking Back）	管理者の要求による	フォールバック中（Falling Back）	管理者の要求による	管理者がノード2からノード1への手動フォールバックを開始しました。手動フォールバックの処理中です。
アイドル（Idle）	初期化	バックアップ モードで実行中（Running in Backup Mode）	管理者の要求による	ノード1が「アイドル」状態のとき、管理者がノード1上でSRMサービスを再起動しました。
アイドル（Idle）	初期化	バックアップ モードで実行中（Running in Backup Mode）	初期化	プレゼンス冗長グループの手動フェールオーバーモードのとき、管理者がプレゼンス冗長グループの両方のノードを再起動したか、両方のノードのSRMサービスを再起動しました。
アイドル（Idle）	管理者の要求による	バックアップ モードで実行中（Running in Backup Mode）	初期化	ノード2がバックアップ モードで実行しているとき、ノード1のハートビートのタイムアウト前に、管理者がノード2のSRMサービスを再起動しました。
フェールオーバー中（Failing Over）	管理者の要求による	テイクオーバー中（Taking Over）	初期化	ノード2のテイクオーバー中、ノード1のハートビートのタイムアウト前に、管理者がノード2のSRMサービスを再起動しました。
テイクバック中（Taking Back）	初期化	フォールバック中（Falling Back）	管理者の要求による	ノード1のテイクバック中、ノード2のハートビートのタイムアウト前に、管理者がノード1のSRMサービスを再起動しました。テイクバック プロセスの完了後、両方のノードは「通常」状態になります。
テイクバック中（Taking Back）	自動フォールバック	フォールバック中（Falling Back）	自動フォールバック	ノード2からノード1への自動フォールバックが開始され、現在処理中です。

ノード1		ノード2		
状態	理由	状態	理由	原因/推奨するアクション
フェールオーバー済み（Failed Over）	初期化または重要なサービスのダウン	バックアップ モードで実行中（Running in Backup Mode）	重要なサービスのダウン	次のいずれかの条件が発生すると、ノード1は「フェールオーバー完了」状態に遷移します。 • ノード1のリブートにより、重要なサービスの状態が元に戻る。 • ノード1が「重要サービスを実行せずにフェールオーバー完了」状態のとき、管理者がノード1で重要なサービスを開始する。 ノード1が「フェールオーバー完了」状態に遷移する際、プレゼンス冗長グループのノードを「通常」状態へ復元するために、管理者がノード1を手動フォールバックできる状態にある。
重要サービスを実行せずにフェールオーバー完了	重要なサービスのダウン	バックアップ モードで実行中（Running in Backup Mode）	重要なサービスのダウン	ノード1で重要なサービスがダウンしました。IM and Presence サービスが、ノード2への自動フェールオーバーを実行します。 **推奨するアクション:** **1.** ノード1でダウンしている重要なサービスを確認し、手動でそのサービスの開始を試みます。 **2.** ノード1の重要なサービスが開始しない場合は、ノード1をリブートします。 **3.** リブート後にすべての重要なサービスが稼働中である場合、手動でフォールバックを実行して、プレゼンス冗長グループ のノードを [Normal（正常）] 状態に復元します。

ノード1		ノード2		
状態	理由	状態	理由	原因/推奨するアクション
重要サービスを実行せずにフェールオーバー完了	データベース障害	バックアップ モードで実行中（Running in Backup Mode）	データベース障害	ノード1のデータベース サービスがダウンしました。IM and Presence サービスが、ノード2への自動フェールオーバーを実行します。 **推奨するアクション：** **1.** ノード1をリブートします。 **2.** リブート後にすべての重要なサービスが稼働中である場合、手動でフォールバックを実行して、プレゼンス冗長グループ のノードを [Normal（正常）] 状態に復元します。
障害モードで実行中（Running in Failed Mode）	重要なサービスの開始に失敗	障害モードで実行中（Running in Failed Mode）	重要なサービスの開始に失敗	他のノードからプレゼンス冗長グループのノードへのテイクバック中は、重要なサービスを開始できません。 **推奨処置。**テイクバック中のノードで、次の操作を実行します。 **1.** ノードにダウンしている重要なサービスがないかどうかを確認します。これらのサービスを手動で開始するには、[プレゼンス冗長グループの設定）Presence Redundancy Group Configuration）] ウィンドウの [回復（Recovery）] をクリックします。 **2.** 重要なサービスが開始されない場合は、ノードをリブートします。 **3.** リブート後にすべての重要なサービスが稼働中である場合、手動でフォールバックを実行して、プレゼンス冗長グループ のノードを [Normal（正常）] 状態に復元します。

ノード1		ノード2		
状態	理由	状態	理由	原因/推奨するアクション
障害モードで実行中（Running in Failed Mode）	重要なサービスのダウン	障害モードで実行中（Running in Failed Mode）	重要なサービスのダウン	バックアップ ノードで重要なサービスがダウンしました。両方のノードが障害状態になります。 **推奨するアクション：** **1.** バックアップ ノードにダウンしている重要なサービスがないかどうかを確認します。これらのサービスを手動で開始するには、[プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウで [回復（Recovery）] をクリックします。 **2.** 重要なサービスが開始されない場合は、ノードをリブートします。
ネットワーク接続が喪失しているか、SRM サービスが実行されていないために、ノード 1 がダウンしました。		バックアップ モードで実行中（Running in Backup Mode）	ピア ダウン	ノード 2 がノード 1 からのハードビートを失いました。IM and Presence サービスが、ノード 2 への自動フェールオーバーを実行します。 **推奨するアクション：** ノード 1 が起動したら、次の操作を実行します。 **1.** プレゼンス冗長グループのノード間のネットワーク接続を確認して修復します。ノード間のネットワーク接続を再確立すると、ノードが失敗状態になる場合があります。正常の状態にノードを復元するには、[プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウの [回復（Recovery）] をクリックします。 **2.** 正常（Normal）状態にプレゼンス冗長グループのノードをリストアするために、SRM サービスを開始し、手動フォールバックを実行します。 **3.** （ノードがダウンしている場合）ノード 1 を修復して電源を入れます。 **4.** ノードが起動中で、すべての重要なサービスが稼働中である場合、手動でフォールバックを実行してプレゼンス冗長グループのノードを [正常（Normal）] 状態に復元します。

ノード1		ノード2		
状態	理由	状態	理由	原因/推奨するアクション
（電源切断、ハードウェア障害、シャットダウン、リブートなどにより）ノード1がダウンしました。		バックアップ モードで実行中（Running in Backup Mode）	ピア リブート	ノード1で次のような条件が発生したため、IM and Presence サービスがノード2への自動フェールオーバーを実行しました。 • ハードウェア障害 • 電源切断 • 再起動 • シャットダウン **推奨するアクション：** **1.** ノード1を修復して電源を入れます。 **2.** ノードが起動中で、すべての重要なサービスが稼働中である場合、手動でフォールバックを実行してプレゼンス冗長グループのノードを [正常（Normal）] 状態に復元します。
重要サービスを実行せずにフェールオーバー完了、またはフェールオーバー完了	初期化	バックアップ モード	初期化中のピア ダウン	起動中、ノード2はノード1を参照しません。 **推奨するアクション：** ノード1が起動してすべての重要なサービスが実行されたら、手動フォールバックを実行してプレゼンス冗長グループのノードを「通常」状態に復元します。
障害モードで実行中（Running in Failed Mode）	Cisco Server Recovery Manager がユーザのテイクオーバーに失敗	障害モードで実行中（Running in Failed Mode）	Cisco Server Recovery Manager がユーザのテイクオーバーに失敗	テイクオーバープロセス中にユーザを移動することはできません。 **推奨するアクション：** データベース エラーの可能性があります。[プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウの [回復（Recovery）] をクリックします。問題が解決しない場合は、ノードをリブートします。

ノード1		ノード2		
状態	理由	状態	理由	原因/推奨するアクション
障害モードで実行中（Running in Failed Mode）	Cisco Server Recovery Manager がユーザのテイクバックに失敗	障害モードで実行中（Running in Failed Mode）	Cisco Server Recovery Manager がユーザのテイクバックに失敗	フォールバック プロセス中にユーザを移動することはできません。 **推奨するアクション：** データベース エラーの可能性があります。[プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウの [回復（Recovery）] をクリックします。問題が解決しない場合は、ノードをリブートします。
障害モードで実行中（Running in Failed Mode）	不明（Unknown）	障害モードで実行中（Running in Failed Mode）	不明（Unknown）	他のノードが失敗状態であるか、内部システム エラーの発生中に、ノードの SRM が再起動しました。 **推奨するアクション：** [プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウの [回復（Recovery）] をクリックします。問題が解決しない場合は、ノードをリブートします。
バックアップのアクティブ化	データベースの自動リカバリに失敗	フェールオーバーがサービスに影響	データベースの自動リカバリに失敗	バックアップ ノードでデータベースがダウンしました。ピア ノードはフェールオーバー モードであり、プレゼンス冗長グループのすべてのユーザをテイクオーバーできます。自動リカバリ操作が自動的に開始され、すべてのユーザはプライマリ ノードに移動します。
バックアップのアクティブ化	データベースの自動リカバリに失敗	フェールオーバーがサービスに影響	重要サービスのダウンの自動リカバリ	バックアップ ノードで重要なサービスがダウンしました。ピア ノードはフェールオーバー モードであり、プレゼンス冗長グループのすべてのユーザをテイクオーバーできます。自動リカバリ操作が自動的に開始され、すべてのユーザはピア ノードに移動します。
不明（Unknown）		不明（Unknown）		ノード状態は不明です。 考えられる原因は、IM and Presence Service ノードで高可用性が適切に有効化されていないことです。 **推奨するアクション：** プレゼンス冗長グループの両方のノードで、Server Recovery Manager サービスを再起動します。

ほぼゼロのダウンタイムへの IM and Presence フェールオーバー拡張

前提条件：

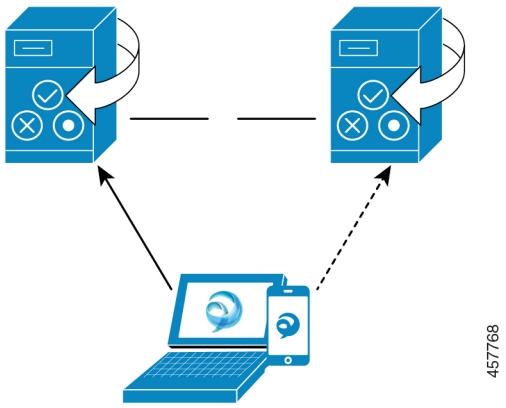
- リリースの互換性：モバイルおよびリモートアクセスユーザの場合、Cisco Unified CM および IM and Presence リリース 14、Jabber リリース 14、および Expressway 14。

IM and Presence サービスは、高可用性フェールオーバーイベント中のサービス停止を排除し、Cisco Jabber クライアントをセカンダリ/バックアップサーバにシームレスに移行できるようにします。

リリース 14 では、IM and Presence サービスは Jabber クライアントとのデュアル接続をサポートしています。このタイプの接続をクライアント側で有効にすると、ハイアベイラビリティフェールオーバーイベント中のサービスダウンタイムが大幅に短縮されます（ほぼゼロ）。

Jabber クライアントでいくつかの追加設定を使用して、この機能を有効にすることができます。Jabber でデュアル接続を有効にする方法の詳細については、『Cisco Jabber 14 のパラメータ リファレンス ガイド』の *EnableDualConnections* および *Inactive_Connection_Activation_Timer* パラメータを参照してください。

図 *2: IM* プレゼンスフェールオーバーの拡張



フェールオーバーの場合、この拡張機能により、ダウンタイムをほぼゼロに最小化できます。これは、Cisco Jabber クライアントが IM and Presence ノードとのデュアル接続を維持できるようにすることで実現されます。クライアントのログインプロセス中に作成されたプライマリノードとのアクティブな接続が維持されます。バックアップノードとの非アクティブな接続は、クライアントの再ログインの下限とクライアントの再ログインの上限の値の間のランダムな秒数後に作成されます。これらの制限は、Cisco Server Recovery Manager サービスのサービスパラメータとして設定されます。

フェールオーバーが発生すると、Jabber クライアントは「非アクティブ」接続をアクティブにしてサーバと通信します。非アクティブな接続がバックアップノードにすでに作成されているため、Jabber のダウンタイムは最小限に抑えられます。

（注） Cisco Jabber クライアントの制限により、このフェールオーバー拡張機能（Jabber 用）は、IM and Presence サービスの無制限（XU）バージョンでは機能しません。これは、無制限バージョンでは Jabber などの XMPP クライアントと IM and Presence サービス間のセキュアな TLS 接続が無効になっているためです。

制限付きバージョンでは、**[セキュリティ設定（Security Settings）]**ページ（**[システム（System）]**> **[セキュリティ（Security）]** > **[設定（Settings）]**）で **[XMPP クライアントから IM/P サービスのセキュア モードを有効にする（Enable XMPP Client to IM/P Service Secure Mod）]** オプションがデフォルトで有効になっており、これにより、フェールオーバー拡張が Jabber で機能するようになります。フェールオーバー拡張を使用する場合は、このモードをオフにしないことをお勧めします。この制限の詳細については、「CSCvx94284」を参照してください。

デュアル登録が成立しているかどうかの確認方法

デュアル登録が確実に確立されるように、プライマリノードに X 人のユーザを割り当て、セカンダリノードに Y 人のユーザを割り当てたシナリオを検討してください。プライマリノードで *JsmSessionsClient* および *JsmSessionsClientInactive* カウンタを確認すると、*JsmSessionsClient* に接続されているユーザの総数が X であり、*JsmSessionsClientInactive* が Y であることがわかります。*JsmSessionsClient* は Y で、*JsmSessionsClientInactive* は X です。

デュアル登録を無効にする方法

サーバの HA を無効にせずにクライアント側の HA を無効にすることで、デュアル登録を無効にすることができます。さらに、HA を無効にすると、サーバからクライアントにデュアル登録が提供されず、クライアントは非アクティブな接続を確立できません。Jabber でデュアル接続を有効にする方法の詳細については、『Cisco Jabber 14 のパラメータ リファレンス ガイド』の *EnableDualConnections* および *Inactive_Connection_Activation_Timer* パラメータを参照してください。

アップグレード中のゼロダウンタイムを監視するカウンタ

ダウンタイムがゼロになるようにアップグレードプロセスを追跡するには、Real-Time Monitoring Tool を使用して次のカウンタを監視します。

表 *6:* アップグレード中のゼロダウンタイムを監視するカウンタ

カウンタ	説明
ActiveJsmSessions	このカウンタは、パブリッシャノードに割り当てられたアクティブユーザの数を提供します。フェールオーバー中、プライマリ（アップグレードされた）ノードにはゼロが表示され、プライマリノードからバックアップノードまでのアクティブユーザが合計されます。

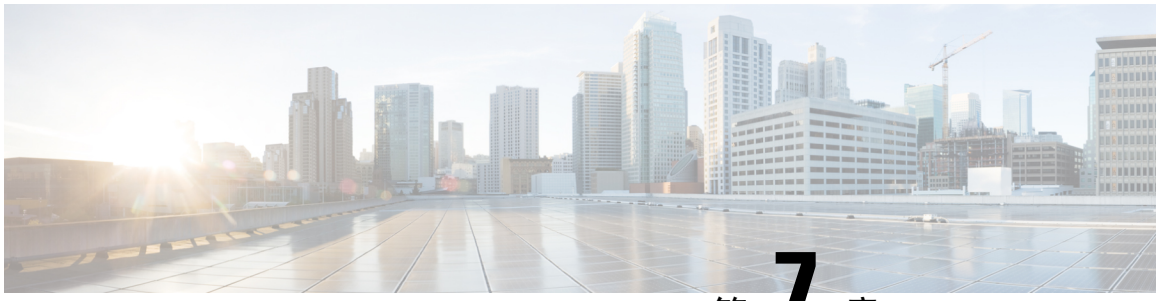
カウンタ	説明
InactiveJsmSessions	このカウンタは、サブスクライバノードに割り当てられたアクティブユーザの数を提供します。
JsmSessionsComposed	このカウンタは、JSM のアクティブな構成済みセッションの数を表します。
JsmSessionsClientInactive	このカウンタは、JSM の非アクティブなクライアントセッションの数を表します。
JsmSessionsClient	このカウンタは、JSM に対してアクティブなクライアントセッションの数を表します。
JsmSessionsClientInactive	このカウンタは、JSM の非アクティブなクライアントセッションの数を表します。

冗長連携動作および制限事項

機能	連携動作
ユーザの追加	いずれかのクラスタ ノードがフェールオーバー状態である間は、IM and Presence Service クラスタに新規ユーザを追加できません。
Multiple Device Messaging	フェールオーバーが発生した場合、Multiple Device Messaging 機能により、IM and Presence サービスでサーバ回復に遅延が発生します。Multiple Device Messaging が設定されているシステムでサーバのフェール オーバーが発生すると、通常、[Cisco Server Recovery Manager] サービス パラメータで指定された時間の 2 倍かかります。

機能	連携動作
プッシュ通知の高可用性	11.5(1)SU3 では、プッシュ通知の展開で高可用性がサポートされます。プッシュ通知が有効化されており、ノードがフェールオーバーした場合、iPhone および iPad 版 Cisco Jabber クライアントで次の処理が行われます。 • フォアグラウンド モードの Cisco Jabber クライアントの場合、Jabber クライアントは、メイン ノードが回復するまでの間、自動的にバックアップ ノードにログインします。バックアップ ノードが引き継いだとき、またはメイン ノードが回復したときのいずれも、サービスは中断しません。 • バックグラウンド モードの Cisco Jabber クライアントの場合、バックアップ ノードが引き継ぎますが、プッシュ通知が送信されるまでに遅延が生じます。Jabber クライアントがバックグラウンド モードで動作しているためにアクティブなネットワーク接続がない場合、バックアップ ノードへのログインは自動的には行われません。バックアップ ノードがプッシュ通知を送信できるようになるには、バックグラウンド モードになっていたすべてのフェールオーバー ユーザ向けに JSM セッションを再作成する必要があります。 遅延の長さは、システムの負荷によって異なります。テストでは、ユーザが HA ペアに均等に分散されている 15,000 ユーザ OVA の場合、フェールオーバー後のプッシュ通知の送信までに 10 ～ 20 分かかることが明らかになっています。この遅延は、バックアップ ノードが引き継いだとき、およびメイン ノードが回復した後に、確認することができます。 （注） ノード障害または予期しない Cisco XCP Router のクラッシュの場合、IM 履歴を含むユーザの IM セッションは、ユーザアクションを必要とすることなく維持されます。ただし、Cisco Jabber on iPhone または iPad のクライアントが保留モードであった場合、サーバのクラッシュ時にサーバ上にキューされていた未開封メッセージを取得することはできません。

機能	連携動作
ユーザの一時的なプレゼンス ステータス	ユーザの一時的なプレゼンス ステータスで、フェールオーバー、フォールバック、およびユーザの移動の後に、古いプレゼンス ステータスが表示されます。これは、一時的なプレゼンスに対するサブスクリプションが削除されたためであり、ユーザの有効な一時的プレゼンス ステータスを表示するためには、ユーザが一時的なプレゼンスに登録し直す必要があります。 たとえば、ユーザ A がユーザ B の一時的なプレゼンスに登録されており、ユーザ B が割り当てられている IM and Presence ノードでフェールオーバーが発生した場合、ユーザ B がバックアップ ノードに再ログインした後でも、ユーザ B はユーザ A に対してオフラインと表示されます。これは、ユーザ B の一時的なプレゼンスに対するサブスクリプションが削除され、ユーザ A が削除を認識していないためです。ユーザ A は、ユーザ B の一時的な存在を再度サブスクライブする必要があります。 ユーザ A が Jabber クライアントから User B の検索を削除すると、ユーザ B の一時的なプレゼンスの検索を試みるまでに、ユーザ A は少なくとも 30 秒待つ必要があります。一致しない場合、ユーザ A にはユーザ B の古いプレゼンスが表示されします。Jabber クライアントは、有効な一時プレゼンス ステータスを取得するために、同じユーザに対する 2 回の検索の間で少なくとも 30 秒待つ必要があります。
IM and Presence ステータス	ユーザーがプレゼンス冗長グループから別のプレゼンスグループに移動した場合、ユーザーが移動した現在のプレゼンス冗長グループで[IM and Presence]ステータスを表示するには、ユーザーが Jabber セッションからログアウトする必要があります。



第 7 章

ユーザ設定値の設定

エンド ユーザ設定の概要

サービス プロファイルや機能グループテンプレートなどのユーザ設定を使用して、LDAP ディレクトリ同期によってエンドユーザに共通設定を適用することができます。LDAP ディレクトリ同期が行われると、設定された設定がすべての同期されたユーザに適用されます。

（注） この章では、IM and Presence Service に適用されるユーザ設定について説明します。ボイスメールや会議などの UC サービスを含む全般的な UC ユーザ設定については、*Cisco Unified Communications Manager* システム設定ガイドの「エンド ユーザの設定」セクションを参照してください。この設定は、LDAP の同期の一部として適用することができます。

サービス プロファイル

サービス プロファイルには、ユニファイド コミュニケーション（UC）サービスの設定が含まれます。異なるユーザ グループ毎に異なるサービスを設定することができるため、各グループのユーザは、業務に合わせて設定された適切なサービスを利用することができます。エンド ユーザが IM and Presence Service を利用することができるには、IM and Presence Service を含めるサービス プロファイルを構成します。

エンド ユーザにサービス プロファイルを適用するには、次の方法を使用します。

- LDAP 同期されたユーザ向け：LDAP ディレクトリからエンドユーザをインポートした場合、サービス プロファイルを機能グループ テンプレートに割り当てることができ、その機能グループテンプレートをエンドユーザに適用することができます。テンプレートの設定は、すべての同期されるユーザに適用されます。

- アクティブなローカル ユーザ（非 LDAP ユーザ）の場合：多数のユーザに一度に設定を適用するには、一括管理ツールを使用して、csv ファイルまたはスプレッドシート経由で、サービス プロファイルの設定を適用します。一括管理ツールの使用方法の詳細は、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlを参照してください。

  あるいは、ユーザ設定を、各ユーザー毎に手動で設定することもできます。

機能グループ テンプレートの概要

機能グループ テンプレートは、LDAP ディレクトリ同期を介してエンドユーザのグループに対して、即座に共通設定を適用する際に役立ちます。たとえば、機能グループ テンプレートを使用して、エンド ユーザに対して IM and Presence Serviceを有効にすることができます。これは、IM and Presence Service が有効にされたプロファイルをテンプレートに適用することで実行可能です。LDAP ディレクトリの同期に機能グループ テンプレートを適用すると、同期が実行される際に、テンプレートからの設定（設定されたサービスプロファイルおよびユーザプロファイル設定を含む) が、すべての同期対象のユーザに適用されます。

機能グループテンプレート設定には、機能グループテンプレートに割り当てられる次のプロファイルが含まれます。

- ユーザプロファイル:一般的な電話機と電話回線の設定のセットが含まれています。共通の電話回線の設定を割り当てるユニバーサル回線テンプレートと、共通の電話回線の設定を割り当てるユニバーサルデバイステンプレートを使用して、ユーザプロファイルを設定する必要があります。これらのテンプレートは、セルフプロビジョニングを設定しているユーザが自分の電話機を設定するのをサポートします。
- サービス プロファイル：IM and Presence Service、ディレクトリ、ボイスメールなど、一般的な UC サービスが含まれます。

ユーザ設定の前提条件

IM and Presence Serviceクラスタ間でユーザを移動する場合は、エンド ユーザを設定する前にユーザを移動する必要があります。Cisco Unified CM IM and Presence 管理を使用してユーザを移行する方法、および連絡先リストをエクスポートまたはインポートする方法の詳細については、を参照してください。

（注） クラスタ間でユーザを移行すると、パーティションイントラドメインフェデレーションのために使用されたユーザ移行ツールと混同しないようにする必要があります。

（注） Cisco Jabber を VPN 経由で接続している場合は、IM and Presence Service と Cisco Jabber クライアント間の TLS ハンドシェイク中に、IM and Presence サーバでクライアントの IP サブネットに対する逆引き参照が実行されます。逆引き参照に失敗すると、クライアントマシンで TLS ハンドシェイクがタイムアウトします。

ユーザ設定タスク フローの設定

これらのタスクを実行して、エンドユーザが IM and Presence Service を有効にするなど、共有サービスおよび機能設定を使用して、ユーザ テンプレートを設定します。LDAP 同期の完了後、テンプレートの設定がエンド ユーザに適用されます。

（注） この章では、IM and Presence Service に適用されるユーザ設定のタスク フローについて説明します。ボイスメールや会議などの UC サービスを含む全般的な UC ユーザ設定については、*Cisco Unified Communications Manager* システム設定ガイドの「エンドユーザの設定」セクションを参照してください。この設定は、LDAP の同期の一部として適用することができます。

手順

	コマンドまたはアクション	目的
Step 1	ユーザ割り当てモードの設定 （82 ページ）	ユーザ割り当てモードを、「バランス」、「アクティブ/スタンバイ」、または「なし」に設定します。
Step 2	IM and Presence UC サービスの追加 （82 ページ）	Cisco Unified Communications Manager で IM and Presence Service をセットアップします。
Step 3	サービス プロファイルの設定 （83 ページ）	追加した IM and Presence UC サービスを含むサービス プロファイルを設定します。
Step 4	機能グループ テンプレートの設定 （83 ページ）	他の共通機能設定に加え、設定したサービス プロファイルを含む機能グループ テンプレートを設定します。

次のタスク

LDAP 同期を完了して、LDAP 同期 ユーザに設定を適用します。

ユーザ割り当てモードの設定

この手順を使用すると、Sync Agent がクラスタ内のノードにユーザを分散させる方法を設定できます。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

Step 2 [ユーザ管理パラメータ（User Management Parameters）] 領域で、[プレゼンスサーバのユーザ割り当てモード（User Assignment Mode for Presence Server）] パラメータに次のいずれかのオプションを選択します。

- [バランス（Balanced）]：このモード（デフォルト）では、ユーザを各サブクラスタのそれぞれのノードに均等に割り当て、各ノードにユーザの合計数が均等に分散するようにします。これがデフォルトのオプションです。
- [アクティブスタンバイ（Active-Standby）]：このモードでは、サブクラスタの最初のノードにすべてのユーザを割り当て、セカンダリ サーバをバックアップのままにします。
- **[なし（None）]**：このモードでは、Sync Agent でクラスタのノードにユーザが割り当てられません。

Step 3 [保存（Save）] をクリックします。

次のタスク

IM and Presence UC サービスの追加 （82 ページ）

IM and Presence UC サービスの追加

Cisco Unified Communications Manager でこの手順を使用して、IM and Presence サービス用の UC サービスを追加します。

手順

Step 1 Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [UCサービス（UC Service）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [UCサービスタイプ（UC Service Type）] ドロップダウンリスト ボックスから、[IM and Presence] を選択します。

Step 4 [製品タイプ（Product Type）] ドロップダウンリスト ボックスから、[Unified CM (IM and Presence)] を選択します。

Step 5 IM and Presence サービスの [名前（Name）] と [説明（Description）] を入力します。

Step 6 [ホスト名/IPアドレス（Hostname/IP Address）] フィールドに、IM and Presence サービスをホストするサーバのホスト名、IP アドレス、または DNS SRV を入力します。

Step 7 [保存（Save）] をクリックします。

次のタスク

IM and Presence サービスのユーザを有効にするには、UC サービスをサービス プロファイルに割り当て、そのプロファイルをユーザに割り当てます。

サービス プロファイルの設定 （83 ページ）。

サービス プロファイルの設定

この手順を使用すると、IM and Presence サービスが含まれるサービス プロファイルを設定できます。

始める前に

IM and Presence UC サービスの追加 （82 ページ）

手順

Step 1 Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [サービスプロファイル（Service Profile）]** を選択します。

Step 2 次のいずれかの操作を実行します。

- **[検索（Find）]** をクリックし、既存のプロファイルを選択します。
- **[新規追加（Add New）]** をクリックし、新規プロファイルを作成します。

Step 3 [IM and Presenceプロファイル（IM and Presence Profile）] セクションで、**プライマリ** IM and Presence サーバを選択します。

Step 4 [サービスプロファイルの設定（Service Profile Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

Step 5 [保存（Save）] をクリックします。

次のタスク

機能グループ テンプレートの設定 （83 ページ）

機能グループ テンプレートの設定

共通の機能設定と、設定した IM and Presence 対応サービス プロファイルを含む機能グループ テンプレートを設定します。

始める前に

サービス プロファイルの設定 （83 ページ）

手順

Step 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [機能グループ テンプレート（Feature Group Template）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 機能グループ テンプレートの [名前（Name）] と [説明（Description）] を入力します。

Step 4 このテンプレートを使用するすべてのユーザのホーム クラスタとしてローカル クラスタを使用する場合は、[ホーム クラスタ（Home Cluster）] チェック ボックスをオンにします。

Step 5 このテンプレートを使用するユーザがインスタント メッセージおよびプレゼンス情報を交換できるようにするには、[Unified CM IM and Presenceのユーザを有効化（Enable User for Unified CM IM and Presence）] チェックボックスをオンにします。

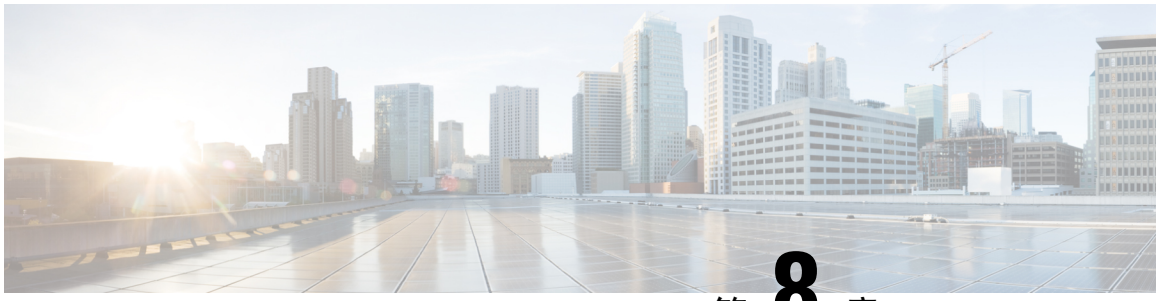
Step 6 ドロップダウン リストから、[サービスプロファイル（Services Profile）] および [ユーザプロファイル（User Profile）] を選択します。

Step 7 [機能グループ テンプレートの設定（Feature Group Template Configuration）] ウィンドウの残りのフィールドに入力します。フィールドの説明については、オンライン ヘルプを参照してください。

Step 8 [保存（Save）] をクリックします。

次のタスク

この機能グループ テンプレートを含む LDAP ディレクトリ同期を設定します。LDAP 同期を完了すると、テンプレート内の IM and Presence の設定が同期済みユーザに適用されます。「LDAP 同期の設定タスクフロー （87 ページ）」を参照してください。



第 8 章

LDAP ディレクトリの設定

LDAP 同期の概要

Lightweight Directory Access Protocol（LDAP）の同期は、システムのエンドユーザのプロビジョニングと設定を支援します。LDAP の同期中、システムは外部 LDAP ディレクトリから Cisco Unified Communications Manager データベースにユーザのリストと関連するユーザ データをインポートします。インポートしている間に、エンドユーザを設定することもできます。

（注） Unified Communication Manager は、LDAPS（SSL を使用した LDAP）をサポートしますが、StartTLS を使用した LDAP はサポートしていません。LDAP サーバ証明書を Unified Communication Manager に Tomcat-Trust 証明書としてアップロードします。

サポートされている LDAP ディレクトリの詳細については、*Cisco Unified Communications Manager と IM and Presence Service* の互換性マトリクスを参照してください。

LDAP 同期では、以下の機能がアドバタイズされます。

- **エンド ユーザのインポート：** LDAP 同期を使用して、システムの初期設定時にユーザ一覧を会社の LDAP ディレクトリから Unified Communication Manager のデータベースにインポートできます。機能グループテンプレート、ユーザプロファイル、サービスプロファイル、ユニバーサルデバイス、回線テンプレートなどの設定項目が設定されている場合は、設定をユーザに適用することができ、また、同期プロセス中に設定したディレクトリ番号とディレクトリ Uri を割り当てることができます。LDAP同期プロセスは、ユーザーリストとユーザー固有のデータをインポートし、設定した構成テンプレートを適用します。

（注） 初期同期が実行された以降は、LDAP 同期を編集することはできません。

- **スケジュールされた更新**：Unified Communication Manager をスケジュールされた間隔で複数の LDAP ディレクトリと同期するように設定できます。これによって確実にデータベースが定期的に更新され、すべてのユーザ データを最新に保ちます。
- **エンドユーザの認証**：LDAP 同期を使用して、システムが Cisco Unified Communications Manager データベースではなく、LDAP ディレクトリに対してエンド ユーザ パスワードを認証するように設定できます。LDAP 認証によって、企業は、すべての企業内アプリケーションに対応する単一のパスワードをエンド ユーザに割り当てることができます。この機能は、PIN またはアプリケーションユーザー パスワードには適用されません。
- **Cisco モバイルおよびリモートアクセス クライアントおよびエンドポイントのディレクトリ サーバユーザ検索**：企業ファイアウォールの外部で操作している場合でも、社内ディレクトリサーバを検索できます。この機能を有効にすると、ユーザデータ サービス（UDS）がプロキシとして機能し、Unified Communication Manager データベースにユーザ検索要求を送信する代わりに、それを社内ディレクトリに送信します。

エンド ユーザ用 LDAP 認証

LDAP 同期を使用して、システムが Cisco Unified Communications Manager データベースではなく、LDAP ディレクトリに対してエンド ユーザ パスワードを認証するように設定できます。LDAP 認証によって、企業は、すべての企業内アプリケーションに対応する単一のパスワードをエンド ユーザに割り当てることができます。この機能は、PIN またはアプリケーションユーザー パスワードには適用されません。

Cisco モバイルおよびリモート アクセス クライアントおよびエンドポイント向けディレクトリ サーバ ユーザ検索

以前のリリースでは、Cisco モバイルおよびリモート アクセス クライアント（たとえば、Cisco Jabber）またはエンドポイント（たとえば、Cisco DX 80 電話）を使用しているユーザが企業ファイアウォールの外部でユーザ検索を実行した場合、結果は Cisco Unified Communications Manager に保存されたユーザ アカウントに基づいていました。データベースには、ローカルで設定されたか、または社内ディレクトリから同期されたユーザ アカウントも含まれています。

このリリースでは、Cisco モバイルおよびリモート アクセス クライアントとエンドポイントは、企業ファイアウォールの外部で動作している場合でも、社内ディレクトリ サーバを検索できます。この機能を有効にすると、ユーザ データ サービス（UDS）がプロキシとして機能し、Cisco Unified Communications Manager データベースにユーザ検索要求を送信する代わりに、それを社内ディレクトリに送信します。

この機能を使用して、次の結果を実現できます。

- 地理的な場所にかかわらず同じユーザ検索結果を配信: 企業ファイアウォール外に接続されている場合でも、モバイルおよびリモート アクセス クライアントとエンドポイントは、社内ディレクトリを使用してユーザ検索を実行できます。

- Cisco Unified Communications Manager データベースに設定されているユーザアカウントの数を減らす: モバイルクライアントが社内ディレクトリ内のユーザを検索できるようになりました。以前のリリースでは、ユーザの検索結果はデータベースに設定されているユーザに基づいています。ユーザの検索に使用するデータベースに対しては、管理者がユーザアカウントを設定または同期する必要がなくなりました。管理者は、クラスタによって提供されているユーザアカウントのみを設定する必要があります。データベース内のユーザアカウントの総数を減らすと、ソフトウェアアップグレードの時間枠が短縮され、データベースの全体的なパフォーマンスが向上します。

この機能を構成するには、**LDAP検索構成ウィンドウ**で**エンタープライズディレクトリサーバー**のユーザー検索を有効にし、LDAPディレクトリサーバーの詳細を構成する必要があります。詳細については、「エンタープライズ ディレクトリ ユーザ検索の設定（93 ページ）」の手順を参照してください。

LDAP 同期の前提条件

前提タスク

LDAP ディレクトリからエンドユーザをインポートする前に、次のタスクを実行します。

- ユーザー アクセスの設定
- クレデンシャル ポリシーの設定
- 機能グループ テンプレートの設定

自分のシステムにデータを同期するユーザについて、アクティブ ディレクトリ サーバ上の電子メール ID フィールドが確実に単一エントリまたは空白になっているようにします。

LDAP 同期の設定タスクフロー

外部 LDAP ディレクトリからユーザ リストをプルし、Unified Communication Manager のデータベースにインポートするには、以下のタスクを使用します。

（注） LDAP ディレクトリをすでに一度同期している場合、外部 LDAP ディレクトリから新しい項目を同期することはできますが、Unified Communication Manager 内の新しい設定を LDAP ディレクトリ同期に追加することはできません。この場合は、一括管理ツールを使用して、ユーザの更新やユーザの挿入などのメニューを使用できます。『*Cisco Unified Communications Manager* 一括アドミニストレーション ガイド』を参照してください。

手順

	コマンドまたはアクション	目的
Step 1	Cisco DirSync サービスの有効化 （88 ページ）	Cisco Unified Serviceability にログインし、Cisco DirSync サービスを有効にします。
Step 2	LDAP ディレクトリ同期の有効化 （89 ページ）	Unified Communication Manager の LDAP ディレクトリ同期を有効化します。
Step 3	LDAP フィルタの作成 （90 ページ）	（**オプション**）Unified Communication Manager に社内 LDAP ディレクトリからユーザのサブセットだけを同期するには、LDAP フィルタを作成します。
Step 4	LDAP ディレクトリの同期の設定 （90 ページ）	アクセス制御グループ、機能グループのテンプレートとプライマリ エクステンションのフィールド設定、LDAP サーバのロケーション、同期スケジュール、および割り当てなどの LDAP ディレクトリ同期を設定します。
Step 5	エンタープライズ ディレクトリ ユーザ検索の設定 （93 ページ）	（**オプション**）エンタープライズ ディレクトリ サーバ ユーザを検索するシステムを設定します。システムの電話機とクライアントをデータベースの代わりにエンタープライズディレクトリ サーバに対してユーザの検索を実行するように設定するには、次の手順に従います。
Step 6	LDAP 認証の設定 （95 ページ）	（**オプション**）エンド ユーザのパスワード認証に LDAP ディレクトリを使用するには、LDAP 認証を設定します。
Step 7	LDAP アグリーメント サービスパラメータのカスタマイズ （96 ページ）	（**オプション**）任意指定の [LDAP同期（LDAP Synchronization）] サービスパラメータを設定します。ほとんどの導入の場合、デフォルト値のままで問題ありません。

Cisco DirSync サービスの有効化

Cisco Unified Serviceability で Cisco DirSync サービスをアクティブ化するには、次の手順を実行します。社内の LDAP ディレクトリからエンドユーザの設定を同期するには、このサービスをアクティブ化する必要があります。

手順

Step 1 Cisco Unified Serviceability から、**[ツール（Tools）]** > **[サービスのアクティブ化（Service Activation）]** を選択します。

Step 2 [サーバ（Server）] ドロップダウンリストからパブリッシャノードを選択します。

Step 3 [**ディレクトリサービス**(Directory Services **)]**の下で、[Cisco DirSync] ラジオボタンをクリックします。

Step 4 [保存（Save）] をクリックします。

LDAP ディレクトリ同期の有効化

エンド ユーザの設定を社内 LDAP ディレクトリから同期させるには、以下の手順で Unified Communication Manager を設定します。

（注） LDAP ディレクトリをすでに一度同期している場合、外部 LDAP ディレクトリから新しい項目を同期することはできますが、Unified Communications Manager 内の新しい設定を LDAP ディレクトリ同期に追加することはできません。また、機能グループテンプレートやユーザプロファイルなどの基になる構成アイテムの編集を追加することもできません。すでに 1 回の LDAP 同期を完了しており、別の設定でユーザを追加する場合は、ユーザの更新やユーザの挿入などの一括管理メニューを使用できます。

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）]** > **[LDAP]** > **[LDAPシステム（LDAP System）]** を選択します。

Step 2 Unified Communications Manager で LDAP ディレクトリからユーザをインポートするには、[LDAP サーバからの同期を有効にする（Enable Synchronizing from LDAP Server）] チェックボックスをオンにします。

Step 3 [LDAPサーバタイプ（LDAP Server Type）] ドロップダウンリストから、使用する LDAP ディレクトリサーバの種類を選択します。

Step 4 [ユーザ IDのLDAP属性（LDAP Attribute for User ID）] ドロップダウンリストで、[エンドユーザの設定（End User Configuration）] ウィンドウの [ユーザID（User ID）] フィールドに関して、Unified Communications Manager で同期する社内 LDAP ディレクトリから属性を選択します。

Step 5 [保存（Save）] をクリックします。

LDAP フィルタの作成

LDAP フィルタを作成することで、LDAP 同期を LDAP ディレクトリからのユーザのサブセットのみに制限することができます。LDAP フィルタを LDAP ディレクトリに適用する場合、Unified Communications Manager は、フィルタに一致するユーザのみを LDAP ディレクトリからインポートします。

（注） LDAP フィルタを設定する場合は、RFC4515 に指定されている LDAP 検索フィルタ標準に準拠する必要があります。

手順

Step 1 Cisco Unified CM Administration で、**[システム（System）] > [LDAP(LDAP)] > [LDAP フィルタ（LDAP Filter）]** を選択します。

Step 2 [新規追加（Add New）] をクリックして、新しい LDAP フィルタを作成します。

Step 3 [フィルタ名（Filter Name）] テキスト ボックスに、LDAP フィルタの名前を入力します。

Step 4 [フィルタ（Filter）] テキスト ボックスに、フィルタを入力します。フィルタは、UTF-8 で最大 1024 文字まで入力できます。また、丸カッコ（ ()）で囲みます。

Step 5 [保存（Save）] をクリックします。

LDAP ディレクトリの同期の設定

LDAP ディレクトリと同期するように Unified Communications Manager を設定するには、この手順を使用します。LDAP ディレクトリの同期により、エンドユーザのデータを外部の LDAP ディレクトリから Unified Communication Manager データベースにインポートして、エンド ユーザの設定ウィンドウに表示することができます。ユニバーサル回線とデバイステンプレートを使用する機能グループテンプレートがセットアップされている場合は、新しくプロビジョニングされるユーザとその内線番号に自動的に設定を割り当てることができます。

ヒント アクセス制御グループまたは機能グループ テンプレートを割り当てる場合は、LDAP フィルタを使用して、インポートを同じ設定要件のユーザ グループに限定できます。

手順

Step 1 Cisco Unified CM Administration で、**[System（システム）] > [LDAP] > [LDAP Directory（LDAP ディレクトリ）]** を選択します。

Step 2 次のいずれかの手順を実行します。

- [検索（Find）] をクリックし、既存の LDAP ディレクトリを選択します。
- [新規追加（Add New）] をクリックして、新しい LDAP ディレクトリを作成します。

Step 3 [LDAPディレクトリの設定（LDAP Directory Configuration）] ウィンドウで、次のように入力します。

a) [LDAP設定名（LDAP Configuration Name）] フィールドで、LDAP ディレクトリに一意の名前を割り当てます。

b) [LDAP マネージャ識別名（LDAP Manager Distinguished Name）] フィールドに、LDAP ディレクトリ サーバにアクセスできるユーザ ID を入力します。

c) パスワードの詳細を入力し、確認します。

d) [LDAPユーザサーチスペース（LDAP User Search Space）] フィールドに、サーチ スペースの詳細を入力します。

e) [ユーザ同期用のLDAPカスタムフィルタ（LDAP Custom Filter for Users Synchronize）] フィールドで、[ユーザのみ（Users Only）] または [ユーザとグループ（Users and Groups）] を選択します。

f) （オプション）特定のプロファイルに適合するユーザのサブセットのみにインポートを限定する場合は、[グループ用LDAPカスタムフィルタ（LDAP Custom Filter for Groups）] ドロップダウンリストから LDAP フィルタを選択します。

Step 4 [LDAPディレクトリ同期スケジュール（LDAP Directory Synchronization Schedule）] フィールドに、外部 LDAP ディレクトリとデータ同期を行うために Unified Communication Manager が使用するスケジュールを作成します。

Step 5 [同期対象の標準ユーザ フィールド（Standard User Fields To Be Synchronized）] セクションを記入します。各エンドユーザのフィールドで、それぞれ LDAP 属性を選択します。同期プロセスが LDAP 属性の値を Unified Communication Manager のエンドユーザ フィールドに割り当てます。

Step 6 URIダイヤリングを展開する場合は、ユーザのプライマリディレクトリURIアドレスに使用されるLDAP属性が割り当てられていることを確認してください。

Step 7 [同期対象のカスタムユーザフィールド（Custom User Fields To Be Synchronized）] セクションで、必要な LDAP 属性を持つカスタムユーザフィールド名を入力します。

Step 8 インポートしたエンドユーザを、インポートしたすべてのエンドユーザに共通するアクセス制御グループに割り当てるには、次の手順を実行します。

a) [アクセス制御グループに追加（Add to Access Control Group）] をクリックします。

b) ポップアップ ウィンドウで、インポートされたエンド ユーザに割り当てる各アクセス制御グループごとに、対応するチェックボックスをオンにします。

c) [選択項目の追加（Add Selected）] をクリックします。

Step 9 機能グループ テンプレートを割り当てる場合は、[機能グループテンプレート（Feature Group Template）] ドロップダウンリストからテンプレートを選択します。

（注） エンドユーザは、そのユーザが存在しない初回のみ、割り当てられた**機能グループテンプレート**と同期されます。既存の [機能グループ テンプレート（Feature Group Template）] が変更され、関連付けられた LDAP の完全同期が実行される場合、変更点は更新されません。

Step 10 インポートされた電話番号にマスクを適用して、プライマリ内線番号を割り当てるには、次の手順を実行します。

a) [挿入されたユーザの新規回線を作成するために、同期された電話番号にマスクを適用する（Apply mask to synced telephone numbers to create a new line for inserted users）] チェックボックスをオンにします。

b) [マスク（Mask）] を入力します。たとえば、インポートされた電話番号が 8889945 である場合、11XX のマスクによって 1145 のプライマリ内線番号が作成されます。

Step 11 電話番号のプールからプライマリ内線番号を割り当てる場合は、次の手順を実行します。

a) [同期された LDAP 電話番号に基づいて作成されなかった場合、プール リストから新しい回線を割り当て（Assign new line from the pool list if one was not created based on a synced LDAP telephone number）] チェック ボックスをオンにします。

b) [DN プールの開始（DN Pool Start）] テキスト ボックスと [DN プールの終了（DN Pool End）] テキスト ボックスに、プライマリ内線番号を選択する電話番号の範囲を入力します。

Step 12 （オプション）Jabber エンドポイント プロビジョニング セクションで、Jabber デバイスを作成する場合は、以下のドロップダウンから自動プロビジョニングに必要な Jabber デバイスを 1 つ選択します：

- Cisco Dual Mode for Android（BOT）
- Cisco Dual Mode for iPhone（TCT）
- Cisco Jabber for Tablet（TAB）
- Cisco Unified Client Services Framework（CSF）

（注） **[LDAPへのライトバック（Write back to LDAP）]**オプションにより、Unified CM から選択されたプライマリ DN を LDAP サーバーにライトバックすることができます。ライトバック可能な LDAP 属性は、**telephoneNumber**、**ipPhone**、および**mobile**です。

Step 13 [LDAPサーバ情報（LDAP Server Information）] セクションで、LDAP サーバのホスト名または IP アドレスを入力します。

Step 14 TLS を使用して LDAP サーバに対するセキュアな接続を作成する場合は、[TLSを使用（Use TLS）] チェックボックスをオンにします。

（注） Tomcat の再起動後にセキュアポートを介してユーザーを同期しようとすると、ユーザーが同期されないことがあります。ユーザーの同期を正常に行うには、Cisco DirSync サービスを再起動する必要があります。

Step 15 [保存（Save）] をクリックします。

Step 16 LDAP 同期を完了させるには、[完全同期を今すぐ実行（Perform Full Sync Now）] をクリックします。それ以外の場合は、スケジュールされた同期を待つことができます。

（注） LDAP で削除されたユーザは、24 時間後に Unified Communications Manager から自動的に削除されます。また、削除されたユーザが次のいずれかのデバイスのモビリティユーザとして設定されている場合、それらの非アクティブデバイスも自動的に削除されます。

- リモート宛先プロファイル
- リモート接続先プロファイルテンプレート
- モバイルスマートクライアント
- CTI リモート デバイス
- Spark リモートデバイス
- Nokia S60
- Cisco Dual Mode for iPhone
- IMS 統合モバイル（ベーシック）
- キャリア統合モバイル
- Cisco Dual Mode for Android

エンタープライズ ディレクトリ ユーザ検索の設定

データベースではなくエンタープライズディレクトリ サーバに対してユーザ検索を実行するように、システムの電話機とクライアントを設定するには、次の手順を使用します。

始める前に

- LDAP ユーザ検索に選択するプライマリ、セカンダリ、および第 3 サーバが Unified Communication Manager のサブスクライバ ノードに到達可能なネットワークにあることを確認します。
- **[システム（System）] > [LDAP] > [LDAPシステム（LDAP System）]** を選択し、[LDAPシステムの設定（LDAP System Configuration）] ウィンドウの [LDAPサーバタイプ（LDAP Server Type）] ドロップダウンリストから LDAP サーバのタイプを設定します。

手順

Step 1 Cisco Unified CM Administration で、**[システム（System）] > [LDAP] > [LDAP 検索（LDAP Search）]** を選択します。

Step 2 エンタープライズLDAPディレクトリ サーバを使用してユーザ検索を実行するには、[エンタープライズ ディレクトリ サーバのユーザ検索を有効にする（Enable user search to Enterprise Directory Server）] チェックボックスをオンにします。

Step 3 [LDAP 検索の設定（LDAP Search Configuration）] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

Step 4 [保存（Save）] をクリックします。

（注） OpenLDAP サーバでルーム オブジェクトとして表される会議室を検索するには、カスタム フィルタを (| (objectClass=intOrgPerson)(objectClass=rooms)) に設定します。これにより、Cisco Jabber クライアントは部屋に関連付けられた名前およびダイヤル番号で会議室を検索できます。

会議室は、ルーム オブジェクトの OpenLDAP サーバに、**givenName**、**sn**、**mail**、**displayName**、または **telephonenumber** の属性が設定されていると検索可能です。

ディレクトリサーバの UDS 検索のための LDAP 属性

次の表に、**ユーザ検索をエンタープライズディレクトリサーバ**に入力可能にするオプションが有効になっているときに、UDSユーザ検索リクエストが使用するLDAP属性を示します。これらのタイプのディレクトリ要求に対しては、UDS はプロキシとして機能し、企業ディレクトリサーバに検索要求をリレーします。

（注） UDSユーザの応答タグは、いずれかのLDAP属性にマップできます。属性のマッピングは、**LDAP サーバタイプ**ドロップダウンリストから選択したオプションによって決定されます。**システム** > **LDAP** > **LDAPシステム設定**ウィンドウからこのドロップダウンリストにアクセスします。

UDS ユーザの応答タグ	LDAP 属性
userName	• samAccountName • uid
firstName	givenName
lastName	sn
middleName	• initials • middleName
nickName	nickName
displayName	displayName
phoneNumber	• telephonenumber • ipPhone
homeNumber	homephone

UDS ユーザの応答タグ	LDAP 属性
mobileNumber	mobile
email	mail
directoryUri	• msRTCSIP-primaryuseraddress • mail
department	• department • 部署番号
manager	manager
title	title
pager	pager

LDAP 認証の設定

LDAP 認証を有効にして、会社の LDAP ディレクトリに割り当てられているパスワードに対してエンドユーザのパスワードが認証されるようにするには、この手順を実行します。この設定は、エンドユーザのパスワードにのみ適用され、エンドユーザの PIN またはアプリケーション ユーザのパスワードには適用されません。

手順

Step 1 Cisco Unified CM Administration で、**[システム（System）] > [LDAP] > [LDAP認証（LDAP Authentication）]** を選択します。

Step 2 [エンドユーザにLDAP認証を使用（Use LDAP Authentication for End Users）] チェックボックスをオンにして、ユーザ認証に LDAP ディレクトリを使用します。

Step 3 [LDAPマネージャ識別名（LDAP Manager Distinguished Name）] フィールドに、LDAP ディレクトリへのアクセス権を持つ LDAP マネージャのユーザ ID を入力します。

Step 4 [パスワードの確認（Confirm Password）] フィールドに、LDAP マネージャのパスワードを入力します。

（注） Unified Communications Manager をリリース 11.5(1)SU2 からリリース 14SU3 以降にアップグレードする場合は、必ず LDAP パスワードを使用してください。

Step 5 [LDAPユーザ検索ベース（LDAP User Search Base）] フィールドに、検索条件を入力します。

Step 6 [LDAPサーバ情報（LDAP Server Information）] セクションで、LDAP サーバのホスト名または IP アドレスを入力します。

Step 7 TLS を使用して LDAP サーバに対するセキュアな接続を作成する場合は、[TLSを使用（Use TLS）] チェックボックスをオンにします。

Step 8 [保存（Save）] をクリックします。

次のタスク

LDAP アグリーメント サービスパラメータのカスタマイズ（96 ページ）

LDAP アグリーメント サービスパラメータのカスタマイズ

LDAP アグリーメントのシステムレベルでの設定をカスタマイズする、任意指定のサービスパラメータを設定するには、この手順を実行します。これらのサービスパラメータを設定しない場合、Unified Communications Manager により、LDAP ディレクトリ統合のデフォルト設定が適用されます。パラメータの説明については、ユーザ インターフェイスでパラメータ名をクリックしてください。

サービスパラメータを使用して次の設定をカスタマイズできます。

- [最大アグリーメント数（Maximum Number of Agreements）]：デフォルト値は 20 です。
- [最大ホスト数（Maximum Number of Hosts）]：デフォルト値は 3 です。
- [ホスト障害時の再試行の遅延（秒）（Retry Delay On Host Failure (secs)）]：ホスト障害のデフォルト値は 5 です。
- [ホストリスト障害時の再試行の遅延（分）（Retry Delay On HotList failure (mins)）]：ホストリスト障害のデフォルト値は 10 です。
- [LDAP接続のタイムアウト（秒）（LDAP Connection Timeouts (secs)）]：デフォルト値は 5 です。
- [遅延同期の開始時間（分）（Delayed Sync Start time (mins)）]：デフォルト値は 5 です。
- [ユーザカスタマーマップの監査時間（User Customer Map Audit Time）]

手順

Step 1 Cisco Unified CM Administration から、**[システム（System）] > [サービスパラメータ（Service Parameters）]** の順に選択します。

Step 2 [サーバ（Server）] ドロップダウンリスト ボックスからパブリッシャノードを選択します。

Step 3 [サービス（Service）] ドロップダウンリスト ボックスから、[Cisco DirSync] を選択します。

Step 4 Cisco DirSyncサービスパラメータの値を設定します。

Step 5 [保存（Save）] をクリックします。

LDAP ディレクトリ サービス パラメータ

サービス パラメータ	説明
最大アグリーメント数	設定可能なLDAPディレクトリの最大数。デフォルトの設定値は20です。
最大ホスト数	フェールオーバー用として設定できるLDAPホスト名の最大数を指定します。デフォルト値は 3 です。
ホスト障害再試行の遅延(secs)	ホストで障害が発生した後、Cisco Unified Communications Managerが最初のLDAPサーバ（ホスト名）への接続を再試行する前の遅延秒数です。デフォルト値は 5 です。
ホストリストの失敗再試行の遅延(mins)	ホスト リストで障害が発生した後、Cisco Unified Communications Manager が設定された各 LDAP サーバ（ホスト名）への接続を再試行する前の遅延分数です。デフォルトは 10 です。
LDAP Connection Timeout (secs)	Cisco Unified Communications Manager が LDAP 接続を確立できる秒数です。指定した時間内に接続を確立できない場合、LDAPサービス プロバイダーは接続試行を中止します。デフォルトは 5 です。
遅延同期の開始間隔(mins)	Cisco DirSync サービスの起動後に、Cisco Unified Communications Manager がディレクトリ同期プロセスを開始するまでの遅延分数です。デフォルトは 5 です。

LDAP 同期済みユーザをローカル ユーザに変換する

LDAPディレクトリとCisco Unified Communications Managerを同期すると、LDAPに同期されたエンドユーザについては、ローカル ユーザに変換しないかぎり、[エンド ユーザの設定（End User Configuration）] ウィンドウ内のフィールドは編集できません。

[エンド ユーザの設定（End User Configuration）] ウィンドウで LDAP 同期ユーザのフィールドを編集するには、そのユーザをローカル ユーザに変換します。ただし、この変換を行うと、Cisco Unified Communications Manager を LDAP ディレクトリと同期したときにエンドユーザが更新されなくなります。

手順

Step 1 Cisco Unified CM Administration で、**[エンド ユーザ（End Users）]**>**[エンド ユーザ管理（End User Management）]** を選択します。

Step 2 [検索（Find）] をクリックして、エンド ユーザを選択します。

Step 3 [ローカル ユーザへの変換（Convert to Local User）] ボタンをクリックします。

Step 4 [エンド ユーザ設定（End User Configuration）] ウィンドウでフィールドを更新します。

Step 5 [保存（Save）] をクリックします。

アクセス制御グループへの LDAP 同期ユーザの割り当て

LDAP と同期するユーザをアクセス制御グループに割り当てるには、次の手順を実行します。

始める前に

エンドユーザと外部 LDAP ディレクトリが同期されるように Cisco Unified Communications Manager を設定する必要があります。

手順

Step 1 Cisco Unified CM Administration で、**[システム（System）] > [LDAP] > [LDAPディレクトリ（LDAP Directory）]** を選択します。

Step 2 [検索（Find）] をクリックし、設定した LDAP ディレクトリを選択します。

Step 3 [アクセス制御グループに追加（Add to Access Control Group）] ボタンをクリックします。

Step 4 この LDAP ディレクトリのエンドユーザに適用するアクセス制御グループを選択します。

Step 5 [選択項目の追加（Add Selected）] をクリックします。

Step 6 [保存（Save）] をクリックします。

Step 7 [完全同期を実施（Perform Full Sync）] をクリックします。
Cisco Unified Communications Manager が外部 LDAP ディレクトリと同期し、同期したユーザが正しいアクセス制御グループに挿入されます。

（注） 同期したユーザは、アクセス制御グループを初めて追加した時にのみ、選択したアクセス グループに挿入されます。完全同期の実行後に LDAP に追加するグループは、同期したユーザに適用されません。

XMPPクライアントにおける連絡先検索のためのLDAPディレクトリ統合

次のトピックでは、サードパーティ製 XMPP クライアントのユーザが LDAP ディレクトリから連絡先を検索および追加できるように IM and Presence Service で LDAP 設定を行う方法について説明します。

IM and Presence Service の JDS コンポーネントは、LDAP ディレクトリとのサードパーティ製 XMPP クライアント通信を処理します。サードパーティ製 XMPP クライアントは、IM and Presence Service の JDS コンポーネントにクエリを送信します。JDS コンポーネントは、プロビジョニングされた LDAP サーバに LDAP クエリを送信し、XMPP クライアントに結果を返します。

ここで説明する設定を実行する前に、XMPP クライアントを Cisco Unified Communications Manager および IM and Presence Service に統合するための設定を実行します。サードパーティ製 XMPP クライアント アプリケーションの統合に関するトピックを参照してください。

図 *3: XMPP* クライアントにおける連絡先検索のための *LDAP* ディレクトリ統合のワークフロー

次のワークフローの図は、XMPP クライアントで連絡先を検索するために LDAP ディレクトリを統合する手順の概要です。

次の表に、XMPP クライアントで連絡先を検索するために LDAP ディレクトリを統合するタスクのリストを示します。詳細な手順については、関連するタスクを参照してください。

表 *7: XMPP* クライアントにおける連絡先検索のための *LDAP* ディレクトリ統合のタスク リスト

タスク	説明
XMPP クライアントの LDAP サーバの名前とアドレスの設定	LDAP サーバと IM and Presence Service の間で SSL を有効にし、セキュア接続を設定していた場合は、ルート CA 証明書を xmpp-trust-certificate として IM and Presence Service にアップロードします。 **ヒント** 証明書のサブジェクト CN は LDAP サーバの FQDN と一致する必要があります。
XMPP クライアントの LDAP 検索の設定	IM and Presence Service でサードパーティ製 XMPP クライアントの連絡先を検索できるように LDAP 検索設定を指定する必要があります。プライマリ LDAP サーバ 1 台とバックアップ LDAP サーバを最大 2 台指定できます。 **ヒント** オプションとして、LDAP サーバから vCard の取得をオンにすることや、vCard を IM and Presence Service のローカル データベースに保存することができます。
Cisco XCP ディレクトリ サービスのオン	サードパーティ製 XMPP クライアントのユーザが LDAP ディレクトリから連絡先を検索および追加できるようにするには、XCP ディレクトリ サービスをオンにする必要があります。 **ヒント** LDAP サーバの設定およびサードパーティ製 XMPP クライアントの LDAP 検索設定を行うまでは、Cisco XCP ディレクトリ サービスをオンにしないでください。そのようにしないと、サービスは実行を停止します。

LDAP アカウント ロックの問題

サードパーティ製 XMPP クライアントに対して設定する LDAP サーバのパスワードを間違って入力し、IM and Presence Service で XCP サービスを再起動すると、JDS コンポーネントは、不正なパスワードで LDAP サーバに複数回サインインしようとします。数回失敗した後でアカウントをロッ

クアウトするように LDAP サーバーが設定されている場合、LDAP サーバーはある時点で JDS コンポーネントをロックアウトする可能性があります。JDS コンポーネントが LDAP に接続する他のアプリケーション（IM and Presence Service で必要とは限らないアプリケーション）と同じ資格情報を使用している場合、これらのアプリケーションも LDAP からロックアウトされます。

この問題を解決するには、既存の LDAP ユーザと同じロールと特権を持つ別のユーザを設定し、JDS だけがこの 2 番目のユーザとしてサインインできるようにします。LDAP サーバに間違ったパスワードを入力した場合は、JDS コンポーネントだけが LDAP サーバからロックアウトされます。

XMPP クライアントの LDAP サーバの名前とアドレスの設定

Secure Socket Layer（SSL）を有効にする場合は、LDAP サーバと IM and Presence Service の間にセキュア接続を設定し、cup-xmpp-trust 証明書としてルート認証局（CA）証明書を IM and Presence Service にアップロードします。証明書のサブジェクト共通名（CN）は、LDAP サーバの完全修飾ドメイン名（FQDN）に一致させる必要があります。

証明書チェーン（ルート ノードから信頼できるノードへの複数の証明書）をインポートする場合は、リーフ ノードを除くチェーン内のすべての証明書をインポートします。たとえば、CA が LDAP サーバの証明書に署名した場合は、CA 証明書のみをインポートし、LDAP サーバの証明書はインポートしません。

IM and Presence Service と Cisco Unified Communications Manager 間の接続が IPv4 であっても、IPv6 を使用して LDAP サーバに接続できます。IPv6 がエンタープライズ パラメータまたは IM and Presence Service ノードの ETH0 のいずれかで無効になった場合でも、そのノードで内部 DNS クエリを実行し、サードパーティ製 XMPP クライアントの外部 LDAP サーバのホスト名が解決可能な IPv6 アドレスであれば、外部 LDAP サーバに接続できます。

ヒント　サードパーティ製クライアントの外部 LDAP サーバのホスト名は [LDAP サーバ - サードパーティ製 XMPP クライアント（LDAP Server - Third-Party XMPP Client）] ウィンドウで設定します。

始める前に

LDAP ディレクトリのホスト名または IP アドレスを取得します。

IPv6 を使用して LDAP サーバに接続する場合は、LDAP サーバを設定する前に、エンタープライズ パラメータと展開内の各 IM and Presence Service ノードの Eth0 で IPv6 を有効にします。

手順

Step 1　**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [アプリケーション（Application）] > [サードパーティ製クライアント（Third-Party Clients）] > [サードパーティ製 LDAP サーバ（Third-Party LDAP Servers）]** を選択します。

Step 2　**[新規追加]** をクリックします。

Step 3　LDAP サーバの ID を入力します。

Step 4 LDAPサーバのホスト名を入力します。

IPv6 接続の場合は、LDAP サーバの IPv6 アドレスを入力できます。

Step 5 TCP または SSL 接続をリッスンする LDAP サーバのポート番号を指定します。

デフォルト ポートは 389 です。SSL を有効にする場合は、ポート 636 を指定します。

Step 6 LDAP サーバのユーザ名とパスワードを指定します。これらの値は、LDAP サーバで設定したクレデンシャルと一致する必要があります。

この情報については、LDAP ディレクトリのマニュアルまたは LDAP ディレクトリの設定を確認してください。

Step 7 SSL を使用して LDAP サーバと通信するには、**[SSL の有効化（Enable SSL）]** をオンにします。

（注） SSL が有効になっている場合、入力する**ホスト名**の値は、LDAP サーバのホスト名または FQDN のいずれかになります。使用される値は、[security certificate **CN**] または [**SAN**] フィールドの値と一致している必要があります。

IP アドレスを使用する必要がある場合は、この値も**CN**フィールドまたは**SAN**フィールドの証明書で使用する必要があります。

Step 8 [保存（Save）] をクリックします。

Step 9 クラスタ内のすべてのノードで Cisco XCP Router サービスを起動します（このサービスがまだ動作していない場合）。

ヒント

- SSL を有効にすると、IM and Presence Service が SSL 接続を確立した後で、SSL 接続の設定およびデータの暗号化と復号化のときにネゴシエーション手順が実行されるため、XMPP の連絡先検索が遅くなる可能性があります。その結果、ユーザが展開内で XMPP の連絡先検索を広範囲に実行する場合、これがシステム全体のパフォーマンスに影響を与えることがあります。
- LDAP サーバの証明書のアップロード後、LDAP サーバのホスト名とポート値で通信を確認するには、証明書インポート ツールを使用できます。**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [証明書インポート ツール（Certificate Import Tool）]** を選択します。
- サードパーティ製 XMPP クライアント用の LDAP サーバの設定を更新した場合は、Cisco XCP ディレクトリ サービスを再起動します。**[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）] > [コントロール センターの機能サービス（Control Center - Feature Services）]** を選択して、このサービスを再起動します。

次のタスク

XMPP クライアントの LDAP 検索の設定に進みます。

XMPP クライアントの LDAP 検索設定

IM and Presence サービスでサードパーティ製 XMPP クライアントの連絡先を検索できるようにする LDAP 検索設定を指定する必要があります。

サードパーティ製 XMPP クライアントは、検索のたびに LDAP サーバに接続します。プライマリサーバへの接続に失敗しすると、XMPP クライアントは最初のバックアップ LDAP サーバを試し、それが使用不可能な場合は、2 番目のバックアップ サーバを試します（以下同様）。システムのフェールオーバー中に処理中の LDAP クエリーがあると、その LDAP クエリーは次に使用可能なサーバで完了します。

オプションで LDAP サーバからの vCard の取得をオンにできます。vCard の取得をオンにした場合：

- 社内 LDAP ディレクトリは vCards を保存します。
- XMPP クライアントが自身の vCard、または連絡先の vCard を検索すると、vCard は JDS サービスによって LDAP から取得されます。
- クライアントは、社内 LDAP ディレクトリを編集することを許可されていないため、自身の vCard を設定または変更できません。

LDAP サーバからの vCard の取得をオフにした場合

- IM and Presence サービスはローカル データベースに vCard を保存します。
- XMPP クライアントが自身の vCard、または連絡先の vCard を検索すると、vCard はローカルの IM and Presence サービス データベースから取得されます。
- クライアントは、自身の vCard を設定または変更できます。

次の表はXMPP クライアントの LDAP 検索の設定の一覧です。

表 *8 : XMPP* クライアントの *LDAP* 検索設定

フィールド	設定
[LDAPサーバタイプ（LDAP Server Type）]	LDAP サーバ タイプをこのリストから選択します。 • Microsoft Active Directory • [汎用ディレクトリ サーバ（Generic Directory Server）]：他のサポートされている LDAP サーバ タイプ（iPlanet、Sun ONE、または OpenLDAP）を使用する場合は、このメニュー項目を選択します。
User Object Class	LDAP サーバ タイプに適切なユーザ オブジェクト クラスの値を入力します。この値は、LDAP サーバで設定されたユーザ オブジェクト クラスの値と一致する必要があります。 Microsoft Active Directory を使用する場合、デフォルト値は [ユーザ（user）] です。
Base Context（ベース コンテキスト）	LDAP サーバに適切なベース コンテキストを入力します。この値は、LDAP サーバの設定済みドメインおよび/または組織構造と一致している必要があります。

フィールド	設定
ユーザ属性	LDAP サーバタイプに適切なユーザ属性値を入力します。この値は、LDAP サーバで設定されたユーザ属性値と一致する必要があります。 Microsoft Active Directory を使用する場合、デフォルト値は [sAMAccountName] です。 ディレクトリ URI IM アドレス スキームが使用され、ディレクトリ URI がメールまたは msRTCSIPPrimaryUserAddress にマッピングされた場合、メールまたは msRTCSIPPrimaryUserAddress はユーザ属性として指定する必要があります。
LDAP Server 1（LDAP サーバ 1）	プライマリ LDAP サーバを選択します。
LDAP Server 2（LDAP サーバ 2）	（任意）バックアップ LDAP サーバを選択します。
LDAP Server 3（LDAP サーバ 3）	（任意）バックアップ LDAP サーバを選択します。

始める前に

XMPP クライアントの LDAP サーバの名前とアドレスを指定します。

手順

Step 1 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）]** > **[アプリケーション（Application）]** > **[サードパーティ クライアント（Third-Party Clients）]** > **[サードパーティ LDAP 設定（Third-Party LDAP Settings）]** を選択します。

Step 2 次の各フィールドに情報を入力します。

Step 3 ユーザが連絡先の vCard を要求し、LDAP サーバから vCard 情報を取得できるようにする場合は、**[LDAP から vCard を作成（Build vCards from LDAP）]** をオンにします。ユーザが連絡先リストに参加するときにクライアントが自動的に vCard を要求できるようにする場合は、チェックボックスをオフのままにします。この場合、クライアントはローカル IM and Presence サービス データベースから vCard 情報を取得します。

Step 4 vCard FN フィールドを作成するために必要な LDAP フィールドを入力します。ユーザが連絡先の vCard を要求すると、クライアントは、vCard FN フィールドの値を使用して連絡先リストに連絡先の名前を表示します。

Step 5 検索可能な LDAP 属性テーブルで、適切な LDAP ユーザ フィールドにクライアント ユーザ フィールドをマッピングします。

Microsoft Active Directory を使用すると、IM and Presence サービスはテーブルにデフォルト属性値を読み込みます。

Step 6 [保存（Save）] をクリックします。

Step 7 Cisco XCP Router サービスを起動します（このサービスがまだ動作していない場合）。

ヒント　サードパーティ製 XMPP クライアント用の LDAP 検索の設定を更新した場合は、Cisco XCP ディレクトリ サービスを再起動します。**[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）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択して、このサービスを再起動します。

次のタスク

Cisco XCP ディレクトリ サービスをオンに設定します。

Cisco XCP ディレクトリ サービスのオン

サードパーティ製 XMPP クライアントのユーザが LDAP ディレクトリから連絡先を検索および追加できるようにするには、Cisco XCP ディレクトリ サービスをオンにする必要があります。クラスタ内のすべてのノードで Cisco XCP ディレクトリ サービスをオンにします。

（注）　LDAP サーバおよびサードパーティ製 XMPP クライアントの LDAP 検索設定を設定するまでは、Cisco XCP ディレクトリ サービスをオンにしないでください。Cisco XCP ディレクトリ サービスをオンにするが、LDAP サーバおよびサードパーティ製 XMPP クライアントの LDAP 検索を設定しない場合、サービスは開始してから再度停止します。

始める前に

LDAP サーバおよびサードパーティ製 XMPP クライアントの LDAP 検索を設定します。

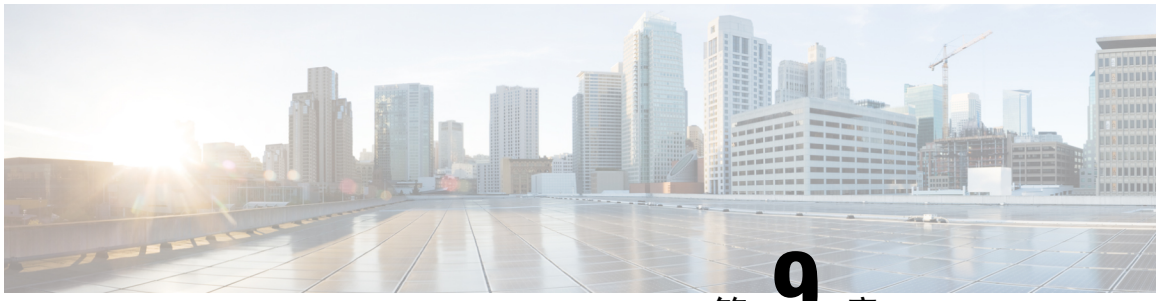
手順

Step 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。

Step 2 [サーバ（Server）] メニューから [IM and Presence サービス（IM and Presence Service）] ノードを選択します。

Step 3 **[Cisco XCP ディレクトリ サービス（Cisco XCP Directory Service）]** を選択します。

Step 4 [保存（Save）] をクリックします。



第 9 章

IM and Presence Service 向けの Cisco Unified Communications Manager の設定

統合の概要

このセクションでは、IM and Presence Service の設定を完了するために、Cisco Unified Communications Manager で完遂するべきタスクの詳細を説明します。

Cisco Unified Communications Manager 統合の前提条件

Cisco Unified Communications Manager にIM and Presence Serviceを統合する設定の前に、Cisco Unified Communications Managerで以下の全般的な設定タスクが完了していることを確認します。Cisco Unified Communications Managerの設定方法の詳細は、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある『*Cisco Unified Communications Manager* システム設定ガイド』を参照してください。

以下の表は、IM and Presence Serviceの統合に関する重要な設定タスクの一覧です。フィールドその他のオプションの説明については、オンライン ヘルプを参照してください。

表 *9 : Cisco Unified Communications Manager* で必要な設定

タスク	説明
ユーザ クレデンシャル ポリシーの修正	ユーザのクレデンシャル ポリシーの有効期限を設定することを推奨します。クレデンシャル ポリシーの有効期限を必要としない唯一のユーザ タイプは、アプリケーション ユーザです。 Cisco Unified Communications Manager は、Cisco Unified Communications Manager のユーザを認証するために LDAP サーバを使用している場合はクレデンシャル ポリシーを使用しません。 **Cisco Unified CM Administration** > **[ユーザの管理（User Management）]** > **[ユーザ設定（User Settings）]** > **[クレデンシャル ポリシー デフォルト（Credential Policy Default）]** を選択します。
電話機を設定し、各電話機に電話番号（DN）を関連付ける	クライアントと電話の相互運用のために、**CTIからのデバイスの制御を許可** を有効にします。 **Cisco Unified CM 管理** > **デバイス** > **電話**
ユーザを設定し、各ユーザにデバイスを関連付ける	ユーザ ID 値が各ユーザで一意になっていることを確認します。 **Cisco Unified CM 管理** > **ユーザ管理** > **エンド ユーザ**
ユーザをラインアピアランスに関連付ける	詳細については、次の項を参照してください。 **Cisco Unified CM 管理** > **デバイス** > **電話**
CTI 対応ユーザ グループにユーザを追加する	デスクフォン制御を有効にするには、CTI 対応ユーザ グループにユーザを追加する必要があります。 **Cisco Unified CM 管理** > **ユーザ 管理** > **ユーザ グループ**
証明書の交換	Cisco Unified Communications Manager と IM and Presence サービスの間の証明書交換は、インストール プロセス中に自動的に処理されます。ただし、問題が発生し、証明書交換を手動で完了しなければならない場合は、Cisco Unified Communications Manager との証明書交換 （156 ページ）を参照してください。

（注） IM and Presence サービスにアップロードする Cisco Unified Communications Manager tomcat の証明書に SAN フィールドのホスト名が含まれている場合は、それらすべてが IM and Presence サービスから解決可能である必要があります。IM and Presence サービスは、DNS を介してホスト名を解決できる必要があります。または、Cisco Sync Agent サービスが開始されません。これは、Cisco Unified Communications Manager サーバのノード名にホスト名、IP アドレス、または FQDN を使用するかどうかにかかわらず当てはまります。

Cisco Unified Communications Manager の SIP トランク設定

Cisco Unified Communications Manager への SIP トランク接続を設定するには、これらのタスクを完了します。

手順

	コマンドまたはアクション	目的
Step 1	SIP トランク セキュリティ プロファイルの設定 （108 ページ）	Cisco Unified Communications Managerと IM and Presence サービスの間のトランク接続用の SIP トランク セキュリティ プロファイルを設定します。
Step 2	IM and Presence Service の SIP トランク セキュリティプロファイルの設定（109ページ）	SIP トランク セキュリティ プロファイルを SIP トランクに割り当て、Cisco Unified Communications Managerと IM and Presence サービスの間のトランクの間の接続を設定します。
Step 3	SRV クラスタ名の設定 （110 ページ）	オプション。Cisco Unified Communications Manager と IM and Presence Service 間で SIP トランクを使用しており、IM and Presence のデフォルト ドメイン以外の SRV アドレスを使用している場合のみ、この手順を実行します。この場合、**SRV クラスタ名**サービス パラメータを設定します。そうしない場合は、このタスクをスキップします。
Step 4	プレゼンス ゲートウェイの設定（111 ページ）	IM and Presence Service で、Cisco Unified Communications Manager をプレゼンス ゲートウェイとして割り当て、システムがプレゼンス情報を交換できるようにします。
Step 5	SIP パブリッシュ トランクの設定 （111 ページ）	オプション。IM and Presence の SIP PUBLISH トランクを設定するには、以下の手順を使用します。この設定をオンにすると、Cisco Unified Communications Manager は、Cisco Unified Communications Manager で IM and Presence Service のライセンスが供与されたユーザに関連付けられたすべてのライン アピアランスの電話の利用状況をパブリッシュします。

	コマンドまたはアクション	目的
Step 6	Cisco Unified Communications Manager のサービスの確認 （112 ページ）	必要なサービスが Cisco Unified Communications Manager で実行されていることを確認します。
Step 7	クラスタ外の Cisco Unified Communications Manager の電話でのプレゼンス表示の設定（112 ページ）	IM and Presence Service の TLS ピア サブジェクトとして、Cisco Unified Communications Manager を設定します。IM and Presence Service クラスタ外の Cisco Unified Communications Manager からの通話のプレゼンスを許可する場合には、TLS が必要となります。

SIP トランク セキュリティ プロファイルの設定

Cisco Unified Communications Manager で、IM and Presence Service のトランク接続用の SIP トランク セキュリティ プロファイルを設定します。

手順

Step 1 **Cisco Unified CM 管理** > **システム** > **セキュリティ** > **SIP トランク セキュリティ プロファイル**で、**検索**をクリックします。

Step 2 **[Non Secure SIP Trunk Profile**（**非セキュアな SIP トランク プロファイル**）**]** をクリックします。

Step 3 [Copy] をクリックします。

Step 4 プロファイルの**名前**を入力します。たとえば、`IMP-SIP-Trunk-Profile`となります。

Step 5 以下の設定を完遂します。

- **デバイス セキュリティ モード** は **非セキュア**に設定されています。
- **着信転送タイプ** は **TCP+UDP**に設定されています。
- **発信転送タイプ** は **TCP**に設定されています。

Step 6 次のチェック ボックスをオンにします。

- **プレゼンスのSUBSCRIBEの許可**
- **Out-of-Dialog REFER の許可**（**Accept Out-of-Dialog REFER**）
- **Unsolicited NOTIFYの許可**
- **[Replacesヘッダーの許可**（**Accept replaces header**）**]**

Step 7 [保存（Save）] をクリックします。

次のタスク

IM and Presence Service の SIP トランク セキュリティ プロファイルの設定 （109 ページ）

IM and Presence Service の SIP トランク セキュリティ プロファイルの設定

Cisco Unified Communications Managerと IM and Presence クラスタの間の SIP トランク接続を設定します。

始める前に

SIP トランク セキュリティ プロファイルの設定 （108 ページ）

手順

Step 1 **Cisco Unified CM 管理**から **デバイス** > **トランク**を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [トランク タイプ（Trunk Type）] ドロップダウン リスト ボックスから、[SIP トランク（SIP Trunk）] を選択します。

Step 4 **デバイス プロトコル** ドロップダウン リスト ボックスから、**SIP** を選択します。

Step 5 **トランク サービス タイプ** ドロップダウン リスト ボックスから、**なし**を選択します。

Step 6 [次へ（Next）] をクリックします。

Step 7 **デバイス名** フィールドに、デバイス名を入力します。たとえば、`IMP-SIP-Trunk`となります。

Step 8 ドロップダウン リスト ボックスから **デバイス プール** を選択します。

Step 9 **SIP 情報** セクションで、IM and Presence クラスタのアドレス情報を入力して、トランクを IM and Presence Service に割り当てます。

- IM and Presence Service に DNS SRV レコードを使用している場合は、**接続先アドレスは SRV** チェック ボックスをオンにして、**接続先アドレス** フィールドに SRV を入力します。
- それ以外の場合は、**[宛先アドレス（Destination Address）]**フィールドに、IM and Presence パブリッシャノードの IP アドレスまたは FQDN を入力します。**(+)** ボタンをクリックして、その他のノードを追加します。最大 16 ノードを入力することができます。

a) **接続先アドレス** フィールドで、IP アドレス、FQDN, あるいは IM and Presence ノードの DNS SRV を入力します。

b) マルチノード展開を設定した場合は、**[Destination Address is an SRV（宛先アドレスはSRVです）]** をオンにします。

このシナリオでは、Cisco Unified Communications Manager は、DNS SRV レコード クエリーを実行して、名前の解決を行います。たとえば、`_sip._tcp.hostname.tld_sip._tcp.hostname.tld` となります。シングル ノード展開を設定する場合は、このチェックボックスをオフのままにすると、Cisco Unified Communications Manager が DNS A レコード クエリーを実行し、名前を解決します。たとえば、`hostname.tld`となります。

DNS SRV レコードの宛先アドレスとして IM and Presence サービスのデフォルト ドメインを使用することを推奨します。

（注） DNS SRV レコードの宛先アドレスとしてドメイン値を指定できます。指定されたドメインにユーザを割り当てる必要はありません。入力したドメイン値が IM and Presence サービスのデフォルト ドメインと異なる場合、IM and Presence サービスの SRV クラスタ名である SIP Proxy サービス パラメータが DNS SRV レコードで指定するドメイン値に一致することを確認する必要がありますデフォルト ドメインを使用する場合は、SRV クラスタ名パラメータの変更は必要ありません。

いずれの場合も、Cisco Unified Communications SIP トランクの宛先アドレスは DNS によって解決し、IM and Presence のノードで設定された SRV クラスタ名に一致する必要があります。

Step 10 **接続先ポート**は、`5060`と入力します。

Step 11 **SIP トランク セキュリティ プロファイル** ドロップダウン リスト ボックスで、前のタスクで作成した SIP トランク セキュリティ プロファイルを選択します。

Step 12 **SIP プロファイル** ドロップダウン リスト ボックスから、プロファイルを選択します。たとえば、**標準 SIP プロファイル**となります。

Step 13 **[保存（Save）]** をクリックします。

次のタスク

Cisco Unified Communications Managerと IM and Presence Service 間で SIP トランクを使用しており、IM and Presence のデフォルト ドメイン以外の SRV アドレスを使用している場合、SRV クラスタ名の設定 （110 ページ）。

それ以外の場合は、SIP パブリッシュ トランクの設定 （111 ページ）.

SRV クラスタ名の設定

Cisco Unified Communications Manager と IM and Presence Service 間で SIP トランクを使用しており、IM and Presence のデフォルト ドメイン以外の SRV アドレスを使用している場合、**SRV クラスタ名** サービス パラメータを設定します。その他の場合は、このタスクをスキップします。

手順

Step 1 Cisco Unified CM IM and Presence 管理で、**システム** > **サービス パラメータ** を選択します。

Step 2 **サーバ** ドロップダウン リスト ボックスから IM and Presence パブリッシャ ノードを選択し、**移動** をクリックします。

Step 3 **サービス** ドロップダウンで、**Cisco SIP プロキシ** サービスを選択します。

Step 4 **SRV クラスタ名** フィールドに、SRV アドレスを入力します。

Step 5 [保存（Save）] をクリックします。

SIP パブリッシュ トランクの設定

このオプション手順を使用して、IM and Presence用の SIP パブリッシュ トランクを設定します。この設定をオンにすると、Cisco Unified Communications Manager は、Cisco Unified Communications Manager で IM and Presence Service のライセンスが供与されたユーザに関連付けられたすべてのライン アピアランスの電話の利用状況をパブリッシュします。

手順

Step 1 Cisco Unified CM IM and Presence 管理で、**プレゼンス** > **設定** > **標準設定**を選択します。

Step 2 **CUCM IM and Presence パブリッシュ トランク** ドロップダウンから、Cisco Unified Communications Manager で IM and Presence Service 用に設定した SIP トランクを選択します。

Step 3 **[保存（Save）]** をクリックします。

（注） この新しい設定を保存すると、Cisco Unified Communications Manager の **IM and Presence パブリッシュ トランク** サービス パラメータにも新しい設定が反映されます。

次のタスク

Cisco Unified Communications Manager のサービスの確認 （112 ページ）

プレゼンス ゲートウェイの設定

IM and Presence Service でこの手順を使用して、Cisco Unified Communications Manager をプレゼンス ゲートウェイとして割り当てます。この設定で、Cisco Unified Communications Manager と IM and Presence Service 間のプレゼンス情報交換が有効になります。

手順

Step 1 **Cisco Unified CM IM and Presence 管理** > **プレゼンス** > **ゲートウェイ**を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 **プレゼンス ゲートウェイ** ドロップダウン リスト ボックスで、**CUCM**を選択します。

Step 4 [説明（Description）] を入力します。

Step 5 **プレゼンス ゲートウェイ タイプ** フィールドから、以下のオプションのいずれかを選択します。

- Cisco Unified Communications Manager パブリッシャ ノードの IP アドレスあるいは FQDN を提供します。
- Cisco Unified Communications Manager サブスクライバ ノードに解決される DNS SRV

Step 6 [保存（Save）] をクリックします。

次のタスク

SIP パブリッシュ トランクの設定 （111 ページ）

Cisco Unified Communications Manager のサービスの確認

この手順を使用して、必要なサービスが Cisco Unified Communications Manager ノードで実行されていることを確認します。

手順

Step 1 Cisco Unified 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）]** の順に選択します。

Step 2 **サーバ** メニューから、Cisco Unified Communications Manager クラスタ ノード を選択kして、**移動** をクリックします。

Step 3 以下のサービスが実行されていることを確認します。実行されていない場合は、起動させます。

- Cisco CallManager
- Cisco TFTP
- Cisco CTIManager
- Cisco AXL Web Service（IM and Presence と Cisco Unified Communications Manager 間のデータ同期用）

Step 4 上記のサービスのいずれかが実行されていない場合は、サービスを選択して、**開始**をクリックします。

クラスタ外の Cisco Unified Communications Manager の電話でのプレゼンス表示の設定

IM and Presence Service クラスタ外にある Cisco Unified Communications Manager から電話利用状況を許可できます。ただし、IM and Presence Service がクラスタ外の Cisco Unified Communications Manager から SIP PUBLISH を受け入れるようにするには、Cisco Unified Communications Manager は、IM and Presence Service の TLS 信頼ピアとしてリストする必要があります。

手順

	コマンドまたはアクション	目的
Step 1	Cisco Unified Communications Manager の TLS ピアとしての追加 （113 ページ）	IM and Presence Service の TLS ピアとして、Cisco Unified Communications Manager を追加します。
Step 2	Unified Communications Manager の TLS コンテキストの設定 （113 ページ）	Cisco Unified Communications Manager TLS ピアの追加

Cisco Unified Communications Manager の TLS ピアとしての追加

IM and Presence Service がクラスタ外の Cisco Unified Communications Manager から SIP PUBLISH を受け入れるようにするには、Cisco Unified Communications Manager は、IM and Presence Service の TLS 信頼ピアとしてリストする必要があります。

手順

Step 1 **Cisco Unified CM IM and Presence 管理** > **システム** > **セキュリティ** > **TLS ピア サブジェクト**で、**新規追加**をクリックします。

Step 2 **ピア サブジェクト名** フィールドに、外部 Cisco Unified Communications Manager の IP アドレスを入力します。

Step 3 **[説明（Description）]** フィールドにノードの名前を入力します。

Step 4 [保存（Save）] をクリックします。

次のタスク

TLS コンテキストの設定 （178 ページ）

Unified Communications Manager の TLS コンテキストの設定

次の手順を使用して、選択した TLS ピアに、前のタスクで設定した Cisco Unified Communications Manager TLS ピアを追加します。

始める前に

Cisco Unified Communications Manager の TLS ピアとしての追加 （113 ページ）

手順

Step 1 **Cisco Unified CM IM and Presence 管理** > **システム** > **セキュリティ** > **TLS コンテクスト設定**で、**検索**をクリックします。

Step 2 **[Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context]** をクリックします。

Step 3 使用可能な TLS ピア サブジェクトのリストから、Cisco Unified Communications Manager 用に設定した TLS ピア サブジェクトを選択します。

Step 4 この TLS ピア サブジェクトを [Selected TLS Peer Subjects] に移動します。

Step 5 [保存（Save）] をクリックします。

Step 6 すべてのクラスタ ノードで Cisco OAMAgent を再起動します。

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** ドロップダウン リスト ボックスから、IM and Presence サーバを選択して、**移動**をクリックします
c) **IM and Presence Services**の下の **Cisco OAMAgent** を選択して、**再起動**をクリックします。
d) すべてのクラスタ ノードでサービスを再起動します。

Step 7 OAM エージェントの再起動後に、Cisco Presence エンジンを再起動します。

a) **[Tools]** > **[Control Center - Feature Services]** を選択します。
b) **サーバ** ドロップダウン リスト ボックスから、IM and Presence ノードを選択して、**移動**をクリックします
c) [IM and Presence サービス（IM and Presence Services）] で、[Cisco Presence Engine] を選択して、[再起動（Restart）] をクリックします。
d) すべてのクラスタ ノードでサービスを再起動します。

次のタスク

Cisco Unified Communications Manager のサービスの確認 （112 ページ）

第 10 章

集中展開の設定

集中展開の概要

IM and Presence の集中展開では、IM and Presence 展開とテレフォニー展開を別々のクラスタに展開できます。中央の IM and Presence クラスタは、企業の IM and Presence を処理し、リモートの Cisco Unified Communications Manager のテレフォニー クラスタは、企業の音声コールおよびビデオ コールを処理します。

集中展開オプションでは、標準展開と比較して次の利点がもたらされます。

- 集中展開オプションでは、IM and Presence サービス クラスタに対して 1x1 の比率のテレフォニー クラスタは必要ありません。IM and Presence 展開とテレフォニー展開をそれぞれ個別のニーズに合わせて拡張できます。
- IM and Presence サービスにフル メッシュ トポロジは必要ありません。
- テレフォニーから独立したバージョン：IM and Presence 集中クラスタは、Cisco Unified Communications Manager のテレフォニー クラスタとは異なるバージョンを実行している可能性があります。
- 中央クラスタから IM and Presence のアップグレードと設定を管理できます。
- コストの低いオプション、特に多数の Cisco Unified Communications Manager クラスタを使用する大規模な展開の場合
- サード パーティとの簡単な XMPP フェデレーション

- Microsoft Outlook との予定表統合をサポート。統合を設定する方法の詳細は、*IM and Presence* サービス との *Microsoft Outlook* 予定表の統合ガイドを参照してください。

OVA 要件

中央集中型の導入の場合は、最小 OVA 15,000 ユーザと、25,000 ユーザ IM and Presence OVA を推奨します。15,000ユーザ OVA は、25000ユーザにまで拡張できます。25K OVA テンプレートと高可用性を有効にした 6 ノード クラスタでは、IM and Presence サービスの中央展開で最大 75,000 のクライアントをサポートしています。25K OVA で 75K ユーザをサポートするには、XCP ルータのデフォルト トレース レベルを **[情報（Info）]** から **[エラー（Error）]** に変更する必要があります。中央クラスタの Unified Communications Manager パブリッシャ ノードでは、次の要件が適用されます。

- 25000 IM and Presence OVA (最大75000ユーザ) は、中央クラスタの Unified Communications Manager パブリッシャ ノードにインストールされた1万ユーザ OVA を使用して展開できます。
- 15000 IM and Presence OVA (最大45,000ユーザ) は、中央クラスタの Unified Communications Manager パブリッシャ ノードにインストールされた 7500 ユーザ OVA を使用して展開できます。

（注） Multiple Device Messaging を有効にする場合は、各ユーザが複数の Jabber クライアントを持つ可能性があるため、ユーザ数ではなくクライアント数に応じた展開にします。たとえば、ユーザ数が 25,000 人で、各ユーザが 2 台の Jabber クライアントを保持している場合、導入環境には 5 万ユーザのキャパシティが必要となります。

集中展開のためのクラスタ間設定

2 つの中央集中型クラスタ間でクラスタ間設定がサポートされています。クラスタ間ピアリング設定は、25K（25K OVA）デバイスを持つ 1 つのクラスタと、15K（15K OVA）デバイスを持つもう 1 つのクラスタでテストされ、パフォーマンス上の問題は見られませんでした。

集中展開のセットアップと標準（非集中型）展開との比較

次の表では、IM and Presence サービスの標準的な展開と比較した、IM and Presence の集中型クラスタ展開の設定の違いについて説明します。

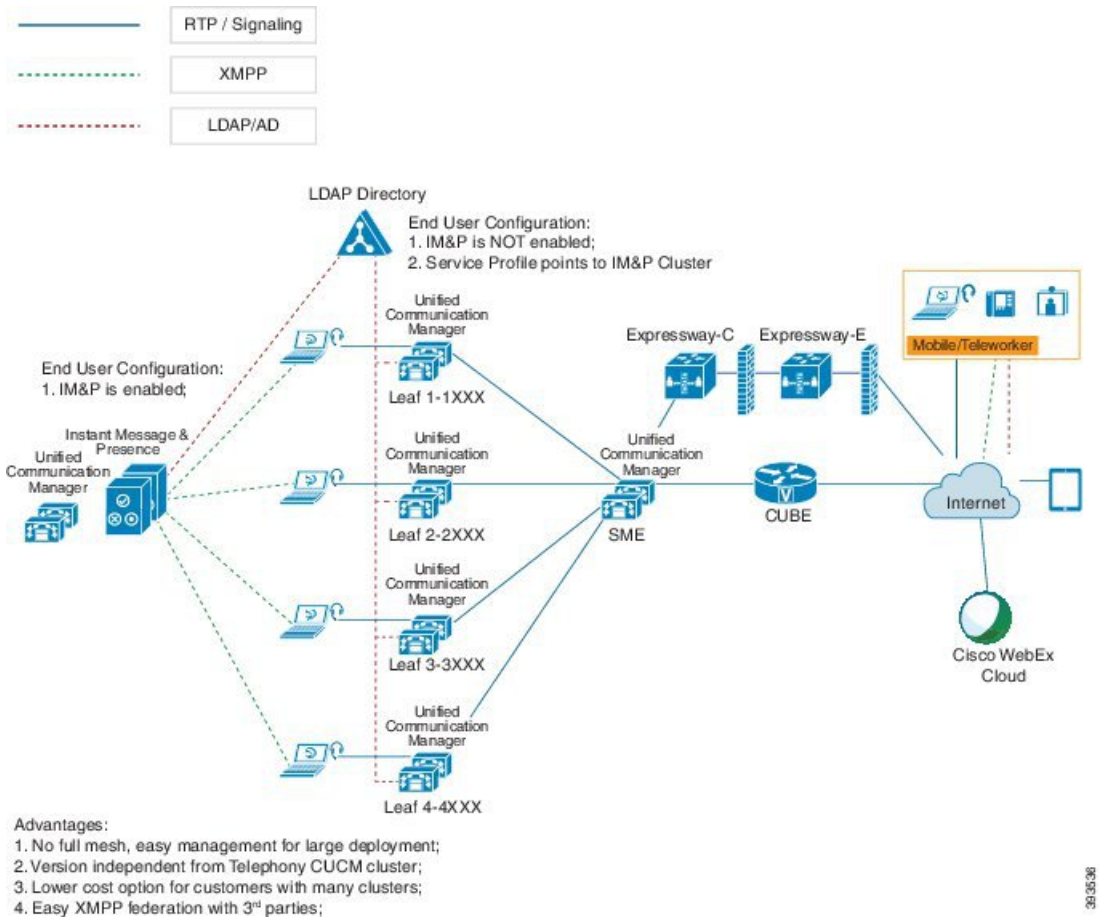
設定段階	標準展開との違い
インストール フェーズ	IM and Presence 中央展開のインストール プロセスは、標準展開と同じです。ただし、中央展開では、IM and Presence 中央クラスタはテレフォニー クラスタとは別にインストールされ、別のハードウェア サーバ上に配置される場合があります。トポロジの計画方法によっては、IM and Presence の中央クラスタをテレフォニー クラスタとは別の物理ハードウェアにインストールすることができます。 IM and Presence の中央クラスタの場合は、引き続き Cisco Unified Communications Manager をインストールしてから、IM and Presence サービスを同じサーバにインストールする必要があります。ただし、IM and Presence の中央クラスタの Cisco Unified Communications Manager インスタンスは、主にデータベースおよびユーザ プロビジョニング用であり、音声コールまたはビデオ コールを処理しません。
設定フェーズ	標準（非集中型）展開と比較すると、IM and Presence サービス の中央展開を設定するには、以下の追加設定が必要となります。 • テレフォニー クラスタと IM and Presence サービスの中央クラスタの両方にユーザを同期させ、両方のデータベースに存在させる必要があります。 • テレフォニー クラスタでは、エンド ユーザを IM and Presence で有効にするべきではありません。 • テレフォニー クラスタでは、サービス プロファイルに IM and Presence サービスが含まれていて、IM and Presence 中央クラスタを指している必要があります。 • IM and Presence 中央クラスタでは、IM and Presence サービスに対してユーザを有効にする必要があります。 • IM and Presence 中央クラスタのデータベース パブリッシャ ノードで、リモート Cisco Unified Communications Manager のテレフォニー クラスタ ピアを追加します。 IM and Presence サービス の標準展開で使用される以下の設定は、集中型展開では必要ありません。 • プレゼンス ゲートウェイは必要ありません。 • SIP パブリッシュ トランクは必要ありません。 • IM and Presence の中央クラスタではサービス プロファイルは必要ありません。サービス プロファイルは、中央クラスタが接続するテレフォニー クラスタで設定されます。

集中型クラスタの展開アーキテクチャ

次の図は、この展開オプションのクラスタ アーキテクチャを示しています。Cisco Jabber クライアントは、音声およびビデオ通話のために複数の Cisco Unified Communications Manager クラスタに接続します。この例では、Cisco Unified Communications Manager のテレフォニー クラスタは、Session Management Edition 展開ではリーフ クラスタです。高度なプレゼンスの場合、Cisco Jabber クライアントは IM and Presence サービス の中央クラスタに接続します。IM and Presence 中央クラスタは、Jabber クライアントのインスタント メッセージおよびプレゼンスを管理します。

（注） IM and Presence クラスタには、Cisco Unified Communications Manager のインスタンスがいまだに含まれています。ただし、このインスタンスは、データベースやユーザ プロビジョニングなどの共有機能を処理するためのもので、テレフォニーを処理するものではありません。

図 *4 : IM and Presence* サービスの集中型クラスタ アーキテクチャ

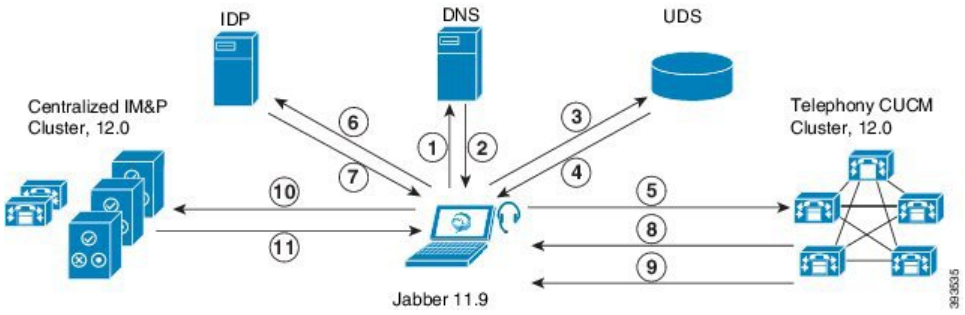


集中型クラスタの使用例

テレフォニーと IM and Presence クラスタを接続するために、アクセス キーを交換するための新しいシステムが導入されています。次の図は、SSO ログインのフローを示しています。

- [1]-[2]：DNS に問い合わせて、SRV レコードを取得します。
- [3]-[4]：UDS に問い合せて、ホームの Cisco Unified Communications Manager クラスタを取得します。
- [5]-[8]：SAML SSO を通じて Cisco Unified Communications Manager クラスタからアクセス トークンと更新トークンを取得します。
- [9]：UC サービス プロファイルを読み取ります。サービス プロファイルは、IM and Presence プロファイルを含み、IM and Presence 中央クラスタを指します。
- [10]：クライアントは、SOAP および XMPP インターフェイスを介して同じアクセス トークンを使用して、IM and Presence クラスタに登録します。
- [11]：トークンが検証され、応答が Jabber クライアントに返されます。

図 *5 : IM and Presence* サービスの集中型クラスタの使用例



集中展開の前提条件

IM and Presence サービス の集中展開には、以下の前提条件が必要です。

- IM and Presence サービス の集中クラスタは、リリース 11.5 SU4 (1) 以降を実行している必要があります。
- IM and Presence の集中クラスタを使用して実行されるローカルの Cisco Unified Communications Manager インスタンスは、IM and Presence の集中クラスタと同じリリースを実行している必要があります。
- リモートの Cisco Unified Communications Manager テレフォニークラスタは、リリース 10.5 (2) 以降を実行している必要があります。
- Cisco Jabber はリリース 11.9 以降で実行されている必要があります。

- プッシュ通知のインスタント メッセージのサポートについては、IM and Presence サービスは、少なくとも 11.5 (1) SU4 を実行している必要があります。
- iOS デバイスのすべてのインスタントメッセージが Apple プッシュ通知サービス（APNs）ソリューションも使用できるように、集中型 IM and Presence クラスタの CUCM パブリッシャ ノードで Cisco Cloud Onboarding を有効にする必要があります。

  さらに、リーフ CUCM クラスタで Cisco Cloud Onboarding オプションを有効にして、通常これらのクラスタに登録する TCT デバイスが、iOS デバイス用の Jabber が一時停止または強制終了されたときに、APN 経由でコールをルーティングできるようにする必要もあります。

  IM and Presence サービスクラスタで Cisco Cloud Onboarding を有効にする方法の詳細については、『プッシュ通知導入ガイド』の「*Enable Cisco Cloud Onboarding*」の章を参照してください。
- Cisco Unified Communications Manager の機能は、IM and Presence 集中クラスタで動作しているローカル インスタンスではなく、リモート テレフォニー クラスタ上で実行されている Cisco ユニファイド コミュニケーション マネージャ のバージョンに依存します。次に例を示します。
  - プッシュ通知のコールをサポートするには、リモートテレフォニークラスタが少なくとも 11.5 (1) SU4 を実行している必要があります。
  - OAuth 更新ログインのサポートについては、リモートの Cisco Unified Communications Manager テレフォニー クラスタは、少なくとも 11.5 (1) SU4 を実行している必要があります。
  - SAML SSO サポートについては、リモート テレフォニー クラスタが少なくとも 11.5 (1) SU4 を実行している必要があります。
- **Cisco AXL Web Service** 機能サービスが、すべてのクラスタで実行されている必要があります。このサービスはデフォルトで有効になっていますが、Cisco Unified Serviceability の [サービスのアクティブ化（Service Activation）] ウィンドウからアクティブになっていることを確認できます。
- 集中型展開では、高度なプレゼンスは Cisco Jabber によって処理されます。ユーザの電話でのプレゼンス表示は、ユーザが Cisco Jabber にログインしている場合にのみ表示されます。

DNS の要件

IM and Presence 集中クラスタが接続する Cisco Unified Communications Manager クラスタのパブリッシャ ノードを指す DNS SRV レコードが必要です。テレフォニー展開に ILS ネットワークが含まれている場合、DNS SRV は、ハブ クラスタを指している必要があります。この DNS SRV レコードは「cisco-uds」を参照している必要があります。

SRV レコードは、特定のサービスをホストするコンピュータの識別に使用されるドメインネームシステム（DNS）リソース レコードです。SRV リソース レコードは、Active Directory のドメイン コントローラの特定に使用されます。ドメイン コントローラの SRV ロケーター リソース レコードを確認するには、以下の方法を使用します。

Active Directory は、以下のフォルダーに SRV レコードを作成します。ドメイン名は、インストールされたドメイン名を表示します。

- 前方参照ゾーン/ドメイン名/_msdcs/dc/_sites/Default-First-Site-Name/_tcp
- 前方参照ゾーン/ドメイン名/_msdcs/dc/_tcp

これらのロケーションには、以下のサービス用のための SRV レコードが表示されます。

- _kerberos
- _ldap
- _cisco_uds : indicates the SRV record

以下のパラメータは、SRV レコードの作成時に設定する必要があります。

- サービス：_cisco-uds
- プロトコル： _tcp
- ウェイト：0から（0 が最優先）
- ポート番号：8443
- ホスト：サーバの FQDN 名

Jabber クライアントを実行しているコンピュータからの DNS SRV レコードの例：

```
nslookup -type=all _cisco-uds._tcp.dcloud.example.com
Server: ad1.dcloud.example.com
Address: x.x.x.x
_cisco-uds._tcp.dcloud.example.com SRV service location:
priority = 10
weight = 10
port = 8443
svr hostname = cucm2.dcloud.example.com
cucm2.dcloud.example.com internet address = x.x.x.y
```

集中展開設定のタスク フロー

新しい IM and Presence の集中型クラスタ展開オプションを構成する場合は、これらのタスクを完了します。

（注） このタスク フローは、新しい IM and Presence サービス を展開する場合にのみ使用します。

表 *10*：集中型クラスタ設定のタスク フロー

	IM and Presence 中央クラスタ	リモート テレフォニー クラスタ	目的
ステップ 1	機能グループ テンプレート経由の IM and Presence の有効化 （123 ページ）		IM and Presence 中央クラスタで、IM and Presence サービスを有効にするテンプレートを構成します。
ステップ 2	IM and Presence 中央クラスタでの LDAP 同期の完了（124 ページ）		LDAP 同期を完了して、IM and Presence 中央クラスタの LDAP 同期ユーザに設定を伝播します。
ステップ 3：	一括管理を介した IM and Presence ユーザの有効化（125 ページ）		オプション。すでに LDAP 同期を完了している場合は、一括管理を使用して、ユーザの IM and Presence を有効にします。
ステップ 4：	リモート テレフォニー クラスタの追加 （126 ページ）		リモート テレフォニー クラスタを IM and Presence 中央クラスタに追加します。
ステップ 5		IM and Presence UC Service の設定 （127 ページ）	テレフォニー クラスタで、IM and Presence 中央クラスタを指す UC サービスを追加します。
ステップ 6：		IM and Presence のサービス プロファイルの作成 （128 ページ）	サービス プロファイルに IM and Presence UC サービスを追加します。Cisco Jabber クライアントはこのプロファイルを使用して、IM and Presence 中央クラスタを検索します。
ステップ 7		テレフォニー クラスタでのプレゼンス ユーザの無効化 （128 ページ）	テレフォニークラスタで、IM and Presence中央クラスタをポイントするプレゼンス ユーザ設定を編集します。
ステップ 8		OAuth 更新ログインの設定 （130 ページ）	テレフォニー クラスタに OAuth を設定すると、集中クラスタの機能が有効になります。

	IM and Presence 中央クラスタ	リモート テレフォニー クラスタ	目的
ステップ 9		ILS ネットワークの設定（130 ページ）	複数のテレフォニー クラスタが存在する場合は、ILS を設定する必要があります。
ステップ 10		モバイルおよびリモート アクセスの設定	集中型展開の場合のモバイルおよびリモートアクセスの設定。

次の作業

- クラスタ間ネットワークの一部として、集中クラスタを別の IM and Presence クラスタに接続する場合は、クラスタ間のピアリングを設定します。
- IM and Presence 管理コンソールで集中型展開に新しいエントリを作成する場合は、Cisco XCP 認証サービスを再起動する必要があります。

機能グループ テンプレート経由の IM and Presence の有効化

この手順で、集中クラスタの IM and Presence の設定を使用して機能グループ テンプレートを設定します。機能グループ テンプレートを LDAP ディレクトリの設定に追加して、同期ユーザに IM and Presence を設定することができます。

（注） 初回同期がまだ行われていない場合にのみ、LDAP ディレクトリ同期に機能グループ テンプレートの編集内容を適用することができます。集中クラスタから LDAP 設定を同期した後は、Cisco Unified Communications Manager の LDAP 設定に編集を適用することはできません。すでにディレクトリを同期している場合は、一括管理を使用して、ユーザの IM and Presence を設定する必要があります。詳細については、一括管理を介した IM and Presence ユーザの有効化（125 ページ）を参照してください。

手順

Step 1 IM and Presence 集中型クラスタの Cisco Unified CM の管理インターフェイスにログインします。このサーバにはテレフォニーが設定されていてはいけません。

Step 2 **[ユーザ管理（User Management）] > [ユーザ電話/追加（User Phone/Add）] > [機能グループテンプレート（Feature Group Template）]** を選択します。

Step 3 次のいずれかを実行します。

- [検索（Find）] をクリックし、既存のテンプレートを選択します。
- [新規追加（Add New）] をクリックして新しいテンプレートを作成します。

Step 4 次の両方のチェックボックスをオンにします。

- **[ホームクラスタ（Home Cluster）]**
- **[Unified CM IM and Presence のユーザを有効にする（Enable User for Unified CM IM and Presence）]**

Step 5 [機能グループ テンプレートの設定（Feature Group Template Configuration）] ウィンドウの残りのフィールドに入力します。フィールドとその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。

Step 6 [保存（Save）] をクリックします。

次のタスク

設定をユーザに適用するには、初期同期がまだ行われていない場合は、機能グループ テンプレートを LDAP ディレクトリの設定に追加してから初期同期を完了する必要があります。

IM and Presence 中央クラスタでの LDAP 同期の完了 （124 ページ）

IM and Presence 中央クラスタでの LDAP 同期の完了

IM and Presence サービスの集中クラスタで LDAP 同期を完了し、機能グループ テンプレートを使用して IM and Presence サービスを持つユーザを設定します。

（注） 初期同期の実行後に、LDAP 同期設定の編集を適用することはできません。初期同期が既に行われている場合には、その代わりに一括管理を使用します。LDAP ディレクトリ同期を設定する方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure End Users」を参照してください。

始める前に

機能グループ テンプレート経由の IM and Presence の有効化 （123 ページ）

手順

Step 1 IM and Presence 集中型クラスタの Cisco Unified CM の管理インターフェイスにログインします。このサーバにはテレフォニーが設定されていてはいけません。

Step 2 **[システム（System）] > [LDAP] > [LDAP ディレクトリ（LDAP Directory）]** の順に選択します。

Step 3 次のいずれかを実行します。

a) [検索（Find）] をクリックし、既存の LDAP ディレクトリ同期を選択します。

b) [新規追加（Add New）] をクリックして、新しい LDAP ディレクトリを作成します。

Step 4 [機能グループテンプレート（Feature Group Template）] ドロップダウン リスト ボックスから、前のタスクで作成した IM and Presence 対応の機能グループ テンプレートを選択します。

Step 5 [LDAPディレクトリ（LDAP Directory）] ウィンドウで残りのフィールドを設定します。フィールドとその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。

Step 6 [保存（Save）] をクリックします。

Step 7 [完全同期を実施（Perform Full Sync）] をクリックします。

Cisco Unified Communications Manager が、データベースを外部の LDAP ディレクトリと同期します。エンド ユーザが、IM and Presence サービスで構成されます。

次のタスク

リモート テレフォニー クラスタの追加 （126 ページ）

一括管理を介した IM and Presence ユーザの有効化

ユーザをすでに中央クラスタに同期させており、それらのユーザが IM and Presence サービスに対して有効になっていない場合は、一括管理の [ユーザの更新(Administration's Update)] 機能を使用して、それらのユーザを IM and Presence サービスに対して有効にします。

（注） 一括管理の [ユーザのインポート(Administration's Import)] または [ユーザの挿入(Insert Users)] 機能を使用して、CSVファイルを介して新しいユーザをインポートすることもできます。手順は、*Cisco Unified Communications Manager* 一括管理ガイドを参照してください。インポートしたユーザ で、下記のオプションが選択されていることを確認します。

- [ホームクラスタ（Home Cluster）]
- [Unified CM IM and Presence のユーザを有効にする（Enable User for Unified CM IM and Presence）]

手順

Step 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）]から、**[一括管理（Bulk Administration）] > [ユーザ（Users）] > [ユーザの更新（Update Users）] > [クエリ（Query）]** の順に選択します。

Step 2 **フィルタ**で、**ホーム クラスタが有効になっている**を選択して、**検索(Find)**をクリックします。このウィンドウには、ここをホーム クラスタとするすべてのエンド ユーザが表示されます。

Step 3 [次へ（Next）] をクリックします。
ユーザ設定の更新 ウィンドウの一番左のチェック ボックスで、この設定をこのクエリで編集するかどうかが表示されます。左側のチェック ボックスをチェックしないと、フィールドはクエリによって更新されません。右側のフィールドは、このフィールドの新しい設定を示しています。2 つのチェック ボックスが表示されている場合は、左側のチェック ボックスをオンにしてフィールドを更新し、右側のチェック ボックスには新しい設定を入力する必要があります。

Step 4 **サービス設定**で、以下の各フィールドの左側のチェックボックスをオンにして、これらのフィールドを更新することを示し、隣接するフィールドの設定を次のように編集します。

- **ホームクラスタ**:このクラスタをホームクラスタとして有効にするには、右側のチェックボックスをオンにします。
- **Unified CM IM and Presence でのユーザの有効化**：右のチェックボックスを確認します。この設定により、中央クラスタがこれらのユーザの IM and Presence サービスのプロバイダーとして有効となります。

Step 5 更新が必要な残りのフィールドをすべて入力します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

Step 6 **ジョブ情報**の下の**今すぐ実行(Run Immediately)**を選択します。

Step 7 [Submit] をクリックします。

リモート テレフォニー クラスタの追加

この手順を使用して、リモート テレフォニー クラスタを集中型 IM and Presence サービス クラスタに追加します。

（注） 複数のテレフォニー クラスタがある場合は、ILS を導入する必要があります。この場合、IM and Presence 集中クラスタが接続するテレフォニー クラスタは、ハブ クラスタでなければなりません。

手順

Step 1 IM and Presence サービスの集中型クラスタでデータベース パブリッシャ ノードにログインします。

Step 2 Cisco Unified CM IM and Presence Administration から、**[システム（System）]**>**[集中展開（Centralized Deployment）]** を選択します。

Step 3 [検索（Find）] をクリックして、現在のリモート Cisco Unified Communications Manager クラスタのリストを表示します。クラスタの詳細を編集する場合は、クラスタを選択し、[Edit Selected] をクリックします。

Step 4 [新規追加（Add New）] をクリックして、新しいリモート Cisco Unified Communications Manager のテレフォニー クラスタを追加します。

Step 5 追加するテレフォニー クラスタごとに、次のフィールドに入力します。

- [ピアアドレス（Peer Address）]：リモート Cisco Unified Communications Manager のテレフォニー クラスタ上のパブリッシャ ノードの FQDN、ホスト名、IPv4 アドレス、または IPv6 アドレス。

- [AXLユーザ名（AXL Username）]：リモート クラスタ上の AXL アカウントのログイン ユーザ名。
- [AXLパスワード（AXL Password）]：リモート クラスタ上の AXL アカウントのパスワード。

Step 6 [保存して同期（Save and Synchronize）] ボタンをクリックします。
IM and Presence サービスが、キーをリモート クラスタと同期させます。

次のタスク

IM and Presence UC Service の設定 （127 ページ）

IM and Presence UC Service の設定

リモート テレフォニー クラスタでこの手順を使用して、IM and Presence サービスの中央クラスタを指す UC サービスを設定します。テレフォニー クラスタのユーザは、IM and Presence 集中クラスタから IM and Presence サービスを取得します。

手順

Step 1 テレフォニー クラスタで Cisco Unified CM の管理インターフェイスにログインします。

Step 2 **[ユーザ管理（User Management）]** > **[ユーザ設定（User Settings）]** > **[UCサービス（UC Service）]** を選択します。

Step 3 次のいずれかを実行します。

a) [検索（Find）] をクリックし、編集する既存のサービスを選択します。

b) [新規追加（Add New）] をクリックして、新しい UC サービスを作成します。

Step 4 [UCサービスタイプ（UC Service Type）] ドロップダウン リスト ボックスから、[IM and Presence] を選択し、[次へ（Next）] をクリックします。

Step 5 [製品タイプ（Product type）] ドロップダウン リスト ボックスから、[IM and Presenceサービス（IM and Presence Service）] を選択します。

Step 6 クラスタの一意の [名前（Name）] を入力します。これはホスト名である必要はありません。

Step 7 **ホスト名 / IP アドレス**で、IM and Presence の集中型クラスタ データベース のパブリッシャ ノードのホスト名、IPv4 アドレス、あるいは IPv6 アドレス を入力します。

Step 8 **[保存（Save）]** をクリックします。

Step 9 推奨。この手順を繰り返して、**ホスト名 / IP アドレス** フィールドが集中クラスタのサブスクライバ ノードを指す 2 番目の IM and Presence サービスを作成します。

次のタスク

IM and Presence のサービス プロファイルの作成 （128 ページ）。

IM and Presence のサービス プロファイルの作成

リモート テレフォニー クラスタでこの手順を使用して、IM and Presence 中央クラスタを指すサービス プロファイルを作成します。テレフォニー クラスタのユーザは、このサービス プロファイルを使用して中央クラスタから IM and Presence サービスを取得します。

手順

Step 1 Cisco Unified CM の管理から、**[ユーザ管理（User Management）]** > **[ユーザ設定（User Settings）]** > **[サービスプロファイル（Service Profile）]** を選択します。

Step 2 次のいずれかを実行します。

a) [検索（Find）] をクリックし、編集する既存のサービス プロファイルを選択します。

b) [新規追加（Add New）] をクリックして、新しいサービス プロファイルを作成します。

Step 3 **IM and Presence Profile** セクションで、以前のタスクで設定した IM and Presence サービスを設定します。

a) **プライマリ** ドロップダウンでデータベース パブリッシャ ノード サービスを選択します。

b) **セカンダリ** ドロップダウンで、サブスクライバ ノード サービスを選択します。

Step 4 [保存（Save）] をクリックします。

次のタスク

テレフォニー クラスタでのプレゼンス ユーザの無効化 （128 ページ）

テレフォニー クラスタでのプレゼンス ユーザの無効化

テレフォニー展開で既に LDAP 同期が完了している場合は、一括管理ツールを使用して、IM and Presence ユーザのテレフォニー クラスタ内のユーザ設定を編集します。この設定では、プレゼンス ユーザが IM and Presence サービス の集中クラスタを指します。

（注） この手順は、テレフォニークラスタのLDAP同期がすでに完了していることを前提としています。ただし、LDAP の初期同期が未完了の場合は、最初の同期にプレゼンス ユーザの集中導入設定を追加することができます。この場合は、テレフォニー クラスタに対して以下の操作を実行します。

- 先ほど設定した**サービス プロファイル**を含む機能グループテンプレートを設定します。**ホーム クラスタ** オプションが選択されていること、**Unified CM IM and Presence のユーザを有効にする** オプションが選択されていないことを確認してください。
- **LDAP ディレクトリ設定**で、**機能グループ テンプレート** を LDAP ディレクトリ同期に追加します。
- 最初の同期を完了します。

機能グループ テンプレートおよび LDAP ディレクトリ同期の設定の詳細は、*Cisco Unified Communications Manager*システム設定ガイドの「エンド ユーザの設定(Configure End Users)」セクションを参照してください。

手順

Step 1 Cisco Unified CM Administration で、**クエリ(Query)** > **一括管理(Bulk Administration)** > **ユーザ(Users)** > **ユーザの更新(Update Users)** > **クエリ(Query)**を選択します。

Step 2 フィルタで、**ホーム クラスタが有効(Home Cluster Enabled)**を選択し、**検索(Find)**をクリックします。このウィンドウには、ここをホームクラスタとするすべてのエンドユーザが表示されます。

Step 3 [次へ（Next）] をクリックします。
ユーザ設定の更新 ウィンドウの一番左のチェックボックスで、この設定をこのクエリで編集するかどうかが表示されます。左側のチェック ボックスをチェックしないと、フィールドはクエリによって更新されません。右側のフィールドは、このフィールドの新しい設定を示しています。2 つのチェックボックスが表示されている場合は、左側のチェックボックスをオンにしてフィールドを更新し、右側のチェック ボックスには新しい設定を入力する必要があります。

Step 4 **サービスの設定**で、以下の各フィールドの左側のチェックボックスをオンにして、これらのフィールドを更新することを示してから、隣の設定を以下に従って編集します。

- **ホーム クラスタ**：ホーム クラスタとしてテレフォニー クラスタを有効にするには、右側のチェック ボックスをオンにします。
- **Unified CM IM and Presence のユーザを有効にする**：右のチェックボックスはオンにしません。この設定では、IM and Presenceのプロバイダーとしてテレフォニー クラスタを無効にします。
- **UC サービス プロファイル**—ドロップ ダウンから、先ほどのタスクで設定したサービス プロファイルを選択します。この設定では、IM およびプレゼンスサービス のプロバイダーとなる IM and Presenceの集中クラスタがユーザに表示されます。

（注） Expressway モバイルおよびリモートアクセスの設定については、https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.htmlにある『*Cisco Expressway* 経由のモバイルおよびリモートアクセス導入ガイド』を参照してください。

Step 5 残りのすべてフィールドの入力を完了します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

Step 6 **ジョブ情報**の下の**今すぐ実行(Run Immediately)**を選択します。

Step 7 [Submit] をクリックします。

次のタスク

OAuth 更新ログインの設定 （130 ページ）

OAuth 更新ログインの設定

テレフォニー クラスタ内の OAuth 更新ログインを有効にします。これで、集中クラスタでこの機能も有効になります。

手順

Step 1 テレフォニー クラスタで Cisco Unified CM 管理にログインします。

Step 2 **[システム（System）]>[エンタープライズ パラメータ（Enterprise Parameters）]** と選択します。

Step 3 **SSO と OAuth の設定** の下で、**更新ログイン フローを使用した OAuth** のエンタープライズ パラメータを **有効**に設定します。

Step 4 パラメータ設定を編集した場合は、**保存（Save）**をクリックします。

（注） OAuth キーが再生成されたら、Jabber OAuth ログインを機能させるために、すべての IM and Presence ノードで Cisco XCP 認証サービスを再起動する必要があります。

ILS ネットワークの設定

リモート テレフォニー クラスタが複数存在する IM and Presence 集中型クラスタでは、クラスタ間検索サービス（ILS）を使用して、IM and Presence 中央クラスタのリモート テレフォニー クラスタをプロビジョニングすることができます。ILS はネットワークを監視し、新しいクラスタやアドレス変更などのネットワーク変更をネットワーク全体に伝播します。

（注） このタスクの流れは、IM and Presence 集中型クラスタの展開に関する ILS 要件に重点を置いています。グローバル ダイヤル プラン レプリケーションや URI ダイヤルの設定など、テレフォニーに関する ILS の追加設定については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure the Dial Plan」を参照してください。

始める前に

ILS を導入する場合は、次のことを確認してください。

- ILS ネットワーク トポロジを計画します。どのテレフォニー クラスタがハブとスポークになるのかを把握する必要があります。
- IM and Presence 中央クラスタが接続するテレフォニー クラスタは、ハブ クラスタでなければなりません。
- ハブ クラスタのパブリッシャ ノードを指す DNS SRV レコードを設定する必要があります。

ILS ネットワークの設計については、http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html で『*Cisco Collaboration System Solution Reference Network Design*』を参照してください。

手順

	コマンドまたはアクション	目的
Step 1	ILS へのクラスタ ID の設定（131 ページ）	テレフォニー クラスタごとに固有のクラスタ ID を設定します。クラスタ ID が `StandAloneCluster`（デフォルト設定）に設定されている間、ILS は機能しません。
Step 2	テレフォニー クラスタでの ILS の有効化（132 ページ）	ILS ネットワーク内の各テレフォニー クラスタのパブリッシャ ノードで ILS を設定およびアクティブ化します。
Step 3	ILS ネットワークが動作していることを確認する（133 ページ）	ILS が動作している場合、使用するテレフォニー クラスタの**ILS 設定** ウィンドウで、「最新」同期ステータスのすべてのリモート クラスタを確認することができます。

ILS へのクラスタ ID の設定

ILS ネットワーク内の各クラスタには、一意のクラスタ ID が必要です。この手順を使用して、テレフォニー クラスタに一意のクラスタ ID を割り当てます。

手順

Step 1 パブリッシャノードで Cisco Unified CM Administration にログインします。

Step 2 **[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** と選択します。

Step 3 [クラスタID（Cluster ID）] パラメータの値を `StandAloneCluster` から設定した一意の値に変更します。クラスタ ID が `StandAloneCluster` の間は、ILS は機能しません。

Step 4 [保存（Save）] をクリックします。

Step 5 ILS ネットワークに参加させる各テレフォニー クラスタのパブリッシャ ノードでこの手順を繰り返します。各クラスタには一意の ID が必要です。

次のタスク

テレフォニー クラスタでの ILS の有効化 （132 ページ）

テレフォニー クラスタでの ILS の有効化

この手順を使用して、Cisco Unified Communications Manager のテレフォニー クラスタで ILS を設定およびアクティブ化します。

（注）
- スポーク クラスタを設定する前に、ハブ クラスタを設定します。
- フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

始める前に

ILS へのクラスタ ID の設定 （131 ページ）

手順

Step 1 テレフォニー クラスタのパブリッシャ ノードで Cisco Unified CM の管理にログインします。

Step 2 **[拡張機能（Advanced Features）] > [ILS設定（ILS Configuration）]** を選択します。

Step 3 [役割（Role）] ドロップダウン リスト ボックスから、設定するクラスタのタイプに応じて、[ハブ クラスタ（Hub Cluster）] または [スポーククラスタ（Spoke Cluster）] を選択します。

Step 4 [リモートクラスタとのグローバルダイヤルプランのレプリケーションデータの交換（Exchange Global Dial Plan Replication Data with Remote Clusters）] チェックボックスをオンにします。

Step 5 [ILS認証の詳細（ILS Authentication Details）] を設定します。

a) さまざまなクラスタ間でTLS認証を使用する場合は、[TLS証明書の使用（Use TLS Certificates）] チェックボックスをオンにします。

（注） TLS を使用する場合は、クラスタ内のノード間で CA 署名付き証明書を交換する必要があります。

b) パスワード認証を使用する場合（TLS を使用するかどうかに関係なく）は、[パスワードの使用（Use Password）] チェックボックスをオンにして、パスワードの詳細を入力します。

Step 6 [保存（Save）] をクリックします。

Step 7 [ILSクラスタ登録（ILS Cluster Registration）] ポップアップで、登録の詳細を設定します。

- [登録サーバ（Registration Server）] テキスト ボックスに、このクラスタに接続するハブ クラスタのパブリッシャノードの IP アドレスまたは FQDN を入力します。これがネットワーク内の最初のハブ クラスタである場合は、このフィールドを空白のままにしておくことができます。
- [このクラスタにあるパブリッシャでクラスタ間検索サービスをアクティブ化（Activate the Intercluster Lookup Service on the publisher in this cluster）] チェックボックスがオンになっていることを確認します。

Step 8 [OK] をクリックします。

Step 9 ILS ネットワークに追加する各テレフォニー クラスタのパブリッシャ ノードでこの手順を繰り返します。
設定した同期値によっては、クラスタ情報がネットワーク全体に伝播する間に遅延が生じることがあります。

クラスタ間で Transport Layer Security（TLS）認証を使用するには、ILS ネットワークの各クラスタのパブリッシャノード間で、Tomcat 証明書を交換する必要があります。Cisco Unified オペレーティング システムの管理から、証明書の一括管理機能を使用して、以下を行います。

- 証明書を各クラスタのパブリッシャノードから中央の場所にエクスポートします
- エクスポートされた証明書を ILS ネットワークに統合します
- ネットワークの各クラスタのパブリッシャノードに証明書をインポートします

詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の「証明書の管理」の章を参照してください。

次のタスク

ILS が稼働し、証明書を交換した後（必要に応じて）、「ILS ネットワークが動作していることを確認する （133 ページ）」に進みます。

ILS ネットワークが動作していることを確認する

この手順を使用して、ILS ネットワークが稼働していることを確認します。

手順

Step 1 任意のテレフォニー クラスタでパブリッシャノードにログインします。

Step 2 Cisco Unified CM Administration から、**[詳細機能（Advanced Features）] > [ILS設定（ILS Configuration）]** を選択します。

Step 3 [ILSクラスタとグローバルダイヤルプランインポート済みカタログ（ILS Clusters and Global Dial Plan Imported Catalogs）] セクションをオンにします。ILS ネットワーク トポロジが表示されます。

モバイルおよびリモート アクセスの設定

Cisco Unified Communications の Mobile & Remote Access は Cisco Collaboration Edge アーキテクチャの中核を成します。Cisco Jabber などのエンド ポイントがエンタープライズ ネットワーク外にある場合、それらのエンド ポイントで、Cisco Unified Communications Manager によって提供される登録、呼制御、プロビジョニング、メッセージングおよびプレゼンス サービスを使用することができます。Expressway は、Unified CM 登録にセキュアなファイアウォール トラバーサルと回線側サポートを提供します。

ソリューション全体で提供されるものは以下の通りです。

1. **オフプレミス アクセス**：企業ネットワーク外においても、Jabber および EX/MX/SX シリーズ クライアントで一貫したエクスペリエンスを提供。
2. **セキュリティ**：セキュアな Business-to-Business（B2B）コミュニケーション
3. **クラウド サービス**：エンタープライズ クラスの柔軟性と拡張性に優れたソリューションにより、Webex の統合とさまざまなサービス プロバイダーに対応
4. **ゲートウェイと相互運用性サービス**：メディアおよびシグナリングの正規化、非標準エンドポイントのサポート

Configuration

すべてのテレフォニーリーフクラスタ上のモバイルおよびリモートアクセスを Expressway-C. で設定するには、**[設定（Configuration）] → [Unified Communications] → [Unified CM Servers]**を選択します。

集中 IM and Presence ノードクラスタ上のモバイルおよびリモートアクセスを Expressway-C. で設定するには、**[設定（Configuration）] → [Unified Communications] → [IM and Presence サービス ノード（IM and Presence Service node）]** を選択します。

モバイルおよびRemote Accessを有効にするには、**設定 → 「モバイルおよびRemote Access」の有効化** を選択して、以下の表に従って制御オプションを選択します。

表 ***11 : OAuth*** 有効化設定

認証パス（Authentication path）	UCM / LADP 基本認証
OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）	オン（On）

OAuth トークンによる承認	オン（On）
ユーザ クレデンシャルによる承認	いいえ（No）
Jabber iOS クライアントによる組み込みの Safari ブラウザの使用の許可	いいえ（No）
内部認証の可用性の確認（Check for internal authentication availability）	はい（Yes）

表 *12 : OAuth* 無効化設定

認証パス（Authentication path）	UCM / LADP 基本認証
OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）	オフ（Off）
ユーザ クレデンシャルによる承認	オン（On）
Jabber iOS クライアントによる組み込みの Safari ブラウザの使用の許可	オフ（Off）
内部認証の可用性の確認（Check for internal authentication availability）	はい（Yes）

（注） モバイルおよびリモートアクセスの基本設定については、次を参照してください。
https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

IM and Presence 中央展開によるアップグレードでは再同期が必要

IM and Presence 集中展開で、IM and Presence 中央クラスタまたはリモート テレフォニー ピア クラスタをアップグレードする場合は、アップグレードが完了した後でクラスタを再同期する必要があります。クラスタ ピアを選択して [保存して同期（Save and Synchronize）] ボタンをクリックすることで、Cisco Unified CM IM and Presence Administration の [集中展開（Centralized Deployment）] ウィンドウからクラスタを再同期できます。

サブドメインの SSO 対応リモート テレフォニー クラスタを使用した IM and Presence 集中型クラスタセットアップ

IM and Presence の集中型展開では、リモート テレフォニー クラスタに複数のサブドメインがある場合、SSO が有効になっているリモートアクセスクライアント（たとえば、Jabber）への SOAP ログインを有効にすることができます。

このセクションでは、SSO 対応のリモートテレフォニークラスタで Jabber へのサブドメインユーザログインを設定する手順について説明します。集中型クラスタと、その集中型クラスタに関連付けられた SSO 対応のリモート テレフォニー クラスタで構成される集中型展開シナリオを検討してください。

サブドメインの SSO 対応ログインを設定するには、次の手順を実行します。

手順

Step 1 Cisco Unified CM の管理にログインして、以下を実行します。

a) LDAP からリーフノードにユーザを同期し、**[ディレクトリ URI（Directory URI）]** フィールドを **[メール ID（Mail ID）]** に設定し、SSO を有効にします。LDAP ユーザを同期する方法については、「LDAP 同期」を参照してください。

b) 同じユーザをリモートテレフォニーノードに同期させ、**ディレクトリ URI** フィールドを**メール ID** に設定します。

c) **[エンドユーザの設定（End User Configuration）]** ページ（**[エンドユーザ（End Users）]** > **[エンドユーザの管理（End User Management）]**）で、IM and Presence ノードに集中クラスタと同じユーザを持たせるために、**[サービス設定（Service Settings）]** の **[Cisco Unified IM and Presence サービスのユーザを有効にする（Enable Users for Cisco Unified IM and Presence Service）（Configure IM and Presence in the associated UC Service Profile）（関連する UC サービスプロファイルで IM and Presence を設定する）]** オプションをオンにします。

d) **[エンドユーザの設定（End User Configuration）]** ページ **([エンドユーザ（End Users）]** > **[エンドユーザの管理（End User Management）])** で、**[権限情報（Permissions Information）]** セクションを使用して、Cisco Call Manager（CCM）エンドユーザグループにユーザを追加します。

e) リモート テレフォニー クラスタで IM and Presence のユーザを無効にします。これを行うには、**[サービス設定（Service Settings）]** の **[Cisco Unified IM and Presence サービスのユーザを有効にする（Enable Users for Cisco Unified IM and Presence Service）（Configure IM and Presence in the associated UC Service Profile）（関連する UC サービスプロファイルで IM and Presence を設定する）]** をオフにします。

f) リモート テレフォニー クラスタの中央クラスタに UC サービスを作成します（**[ユーザ管理（User Management）]** > **[ユーザ設定（User Settings）]** > **[UC サービスの設定（UC Service Configuration）]**）。

g) 中央クラスタでサービスプロファイルを作成し、これをシステムのデフォルトのサービスプロファイルとして設定し、IM and Presence ノードを IM and Presence プロファイルに追加します（**[ユーザ管理（User Management）]** > **[ユーザ設定（User Settings）]** > **[サービスプロファイル（Service Profile）]**）。

h) 中央クラスタで、**[更新ログインフローを使用した OAuth（OAuth with Refresh Login Flow）]** を有効にします。**[エンタープライズパラメータの設定（Enterprise Parameter Configuration）]** ページで、**[更新ログインフローを使用した OAuth（OAuth with Refresh Login Flow）]** パラメータを **[有効（Enabled）]** に設定します。

Step 2 Cisco Unified IM and Presence 管理コンソールにログインし、リーフノードを IM and Presence サービスノードに追加します（**[システム（System）]** > **[集中展開（Centralized Deployment）]**）。

中央集中型展開での電話プレゼンスの統合

集中型展開では、集中型 IM and Presence ノードで複数の SIP トランクを設定することにより、リモート Unified CM クラスタから電話のプレゼンス情報を取得できます。

1 つの Unified CM クラスタのみをプレゼンスゲートウェイとして設定できる標準の展開とは異なり、集中化された展開ではシステムによってこの制限が解除されます。これにより、管理者は複数の CUCM クラスタを IM and Presence ノードのプレゼンスゲートウェイとして追加できます。これは、リモート Unified CM クラスタから電話のプレゼンス情報を取得するのに役立ちます。

次の手順では、リモート Cisco Unified CM クラスタおよび対応する IM and Presence ノードで SIP トランクおよびその他の追加設定を設定する手順を示します。

手順

Step 1 **Cisco Unified CM の管理**のユーザインターフェイスから、以下を行います。

a) **[デバイス（Device）]** > **[トランク（Trunk）]** の順に選択します。新しい SIP トランクを追加し、IM and Presence パブリッシャノードをリーフクラスタとしてポイントします。

b) **[システム]** > **[サービスパラメータの設定（System Service Parameter Configuration）]** を選択し、**[CallManager]** を選択します。**[IM and Presence パブリッシュトランク（IM and Presence Publish Trunk）]** フィールドに、前のステップで追加したリーフクラスタトランクの IP アドレスを入力します。

c) クラスタで使用可能なすべてのユーザのプレゼンスを有効にします。バックエンドの BAT ファイルを使用して、**[エンド ユーザの設定（End User Configuration）]** ページで、すべてのユーザの **[Unified CM IM and Presence のユーザを有効にする（関連付けられた UC サービス プロファイルで IM and Presence を設定する）（Enable user for Unified CM IM and Presence（Configure IM and Presence in the associated UC service profile））]** チェックボックスを 1 回の試行で設定できます。

Step 2 **[Cisco Unified CM IM and Presence の管理]**から、以下を実行します。

a) **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）]** ユーザインターフェイスで、**[プレゼンス（Presence）]** > **[プレゼンスゲートウェイ（Presence Gateway）]**を選択し、ドロップダウンリストからリモート CUCM クラスタの IP アドレスを選択します。

（注） **Centralized Deployment** ページから削除する前に、**[Presence Gateway Configuration]** ウィンドウからリモート Unified CM クラスタを削除してください。

Centralized Deployment ページでリモート CUCM クラスタアドレスを更新するには、次の手順を実行する必要があります。

- **[プレゼンスゲートウェイの設定（Presence Gateway Configuration）]** ウィンドウからリモート CUCM クラスタを削除します。
- **Centralized Deployment ページ**で CUCM アドレスを編集します。

.

- **[Presence Gateway Configuration]** ウィンドウで Unified CM クラスタを再度追加します。

b) **[システム（System）]** > **[セキュリティ（Security）]** > **[着信ACL（Incoming ACL）]**を選択し、リモート Cisco Unified CM の IP アドレスを追加して新しい ACL を作成します。

重要 このノートは、リリース 14SU1 以降に適用されます。

（注） IM and Presence が SIP メッセージのパブリッシュを予期しているすべてのリモート Cisco Unified CM（パブリッシャおよびサブスクライバ）ノードの IP アドレスを追加して新しい着信 ACL を作成します。

c) **[システム（System）]** > **[セキュリティ（Security）]** > **[TLS ピアサブジェクト（TLS Peer Subject）]** を選択し、リモート Cisco Unified CM の IP アドレスを追加します。

重要 このノートは、リリース 14SU1 以降に適用されます。

（注） TLS ピアサブジェクトを作成し、IM and Presence が SIP メッセージのパブリッシュを予期しているすべてのリモート Cisco Unified CM（パブリッシャおよびサブスクライバ）ノードの IP アドレスを追加します。

d) **[システム（System）]** > **[システム（System）]** > **[TLS コンテキスト設定（TLS Context Configuration）]**を選択します。**[TLS ピアサブジェクトマッピング（TLS Peer Subject Mapping）]** セクションで、前のステップでリモート Cisco Unified CM 用に作成された TLS ピアサブジェクトを **[利用可能な TLS ピアサブジェクト（Available TLS Peer Subject）]** ボックスから選択し、それを **[選択された TLS ピアサブジェクト（Selected TLS Peer Subject）]** ボックスに移動します。

Step 3 すべてのクラスタノードで **Cisco OAMAgent** を再起動します。

Step 4 **Cisco Presence Engine** を再起動します。

（注） IM and Presence サービスの集中型展開では、Cisco Jabber のステータスを**サイレント**（**DND**）に変更できます。同じステータスが、制御対象の Cisco IP Phone および Jabber デバイスに反映されます。ただし、集中型展開で複数のデバイスが同じディレクトリ番（DN）で設定されている共有回線の場合、DND ステータスの変更は反映されません。

集中型の導入の相互作用および制限事項

機能	連携動作
ILS ハブ クラスタ	ILS ハブ クラスタがダウンしており、複数のテレフォニークラスタが存在する場合、集中クラスタ機能は動作しません。
ILS の展開	IM and Presence 集中クラスタを使用しており、ILS も導入している場合は、ILS をテレフォニー クラスタに導入することもできます。IM and Presence クラスタ用の Cisco Unified Communications Manager のインスタンスでは、ILS を展開することはできません。このインスタンスは、プロビジョニングのためのもので、テレフォニーを処理するものではありません。
高度なプレゼンス	集中型展開では、ユーザのリッチプレゼンスが Cisco Jabber によって計算されます。ユーザのテレフォニー プレゼンスは、ユーザが Jabber にログインしている場合にのみ表示されます。
Unified Communications Manager のクラスタ ID。	集中型展開では、統合コミュニケーションマネージャークラスタステータスが**OAuth 更新ログインの同期**として表示されます。この機能は、11.5 (1) の SU3 以降で利用可能です。 Unified Communications Manager を 11.5 (1) SU3 またはそれ以前のリリースに追加すると、OAuth 更新ログインがサポートされないため、Cisco Unified CM IM and Presence の**システム** > **集中展開** では、クラスタ ステータスが「未同期」として表示されます。これらのクラスタは、SSO または LDAP ディレクトリ クレデンシャルを使用した IM and Presence サービス の集中型展開に対応しています。 （注） Cisco Jabber のユーザ ログインには機能上の影響はありません。

第 11 章

高度なルーティングの設定

高度なルーティングの概要

以下の接続タイプをシステムが確立する際の方法を指定するには、高度なルーティングを設定します。

- クラスタ内のIM and Presence Service ノード間のクラスタ内接続。
- 同じプレゼンス ドメインを共有する IM and Presence Service クラスタ間のクラスタ間接続。
- 異なるプレゼンス ドメイン間のフェデレーション接続のSIP スタティック ルート。スタティック ルートは、固定パスであり、ダイナミック ルートよりも優先されます。

クラスタ内およびクラスタ間

クラスタ間接続およびクラスタ内接続を確立する 2 つのモード：

- マルチキャスト DNS（MDNS）：MDNS ルーティングは DNS レコードを使用してノード間の接続をセットアップします。クラスタ内のすべてのノードが同じマルチキャスト ドメイン内に存在する場合、MDNS ルーティングを使用することができます。
- ルータ間（デフォルト オプション）：ルータ間接続では、IP アドレスとユーザ情報を使用して、ノード間の接続をダイナミックに構成します。クラスタ内のノードが同じマルチキャスト ドメイン内にない場合、または別のサブネットにある場合に、ルータ間接続を使用します。

（注） XCP ルート ファブリックに参加する新しい XCP ルータをシームレスにサポートできるため、MDNS ルーティングが推奨されます。

高度なルーティングの要件

ルーティングの設定する前に、システムがこういった要件を満たしていることを確認してください。この要件は、MDNS ルーティングまたはルータ間といった使用するルーティング方法の種類によって異なります。

MDNS ルーティングの要件

要件：

- IOS ネットワークで設定されているマルチ キャスト DNS を使用する必要があります。ネットワークでマルチキャスト DNS を無効にすると、MDNS パケットはクラスタ内の他のノードに到達できません。マルチキャストがデフォルトで有効に設定されていたり、ネットワーク内の特定領域で有効になっているネットワークもあります。たとえば、クラスタ ノードを含む領域で有効になっている場合もあります。このようなネットワークでは、MDNS ルーティングを使用するために、ネットワークで追加設定を行う必要はありません。ネットワークでマルチキャスト DNS が無効になっている場合、MDNS ルーティングを使用するには、ネットワーク機器の設定変更を実行する必要があります。
- すべてのノードが同じマルチキャスト ドメイン内にあることを確認します。

ルータ間ルーティングの前提条件

ネットワーク内で使用可能な DNS の場合、クラスタノード名に IP アドレス、ホスト名、または Fqdn を使用できます。ただし、ネットワーク内で DNS が利用できない場合は、ノード名に IP アドレスを使用する必要があります。

ノード名に IP アドレスを使用するようにリセットする必要がある場合は、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlの *Cisco Unified Communications Manager* および *IM and Presence Service* の *IP* アドレスとホスト名変更ガイド の「ノード名の変更」のトピックを参照してください。

高度ルーティング設定のタスク フロー

手順

	コマンドまたはアクション	目的
Step 1	ルーティング通信方法の設定 （143 ページ）	IM and Presence Service がクラスタ ノード間のルータ接続を確立するために使用するルーティング方法は、ルーティングの通信タイプによって決定されます。単一ノードの IM and Presence Service 展開の場合は、

	コマンドまたはアクション	目的
		ルーティング通信タイプをデフォルト設定のままにすることを推奨します。
Step 2	Cisco XCP ルータの再起動（144 ページ）	ルーティングの通信タイプを編集した場合は、Cisco XCP ルータを再起動する必要があります。
Step 3	セキュアなルータ間コミュニケーションの設定（145 ページ）。	オプション。ルータ間通信が設定されている場合は、同じクラスタまたは異なるクラスタ内の XMPP ルータ間でセキュア TLS 接続を設定することができます。 （注） このオプションはパフォーマンスが低下する可能性があります。IM and Presence Service がセキュリティ保護されていないネットワーク上で実行されている場合にのみ有効にしてください。
Step 4	クラスタ ID の設定（146 ページ）	MDNS ルーティングを使用する場合は、クラスタ ID がクラスタ内のすべてのノードで共有されていること、また、その値がクラスタ内で一意であることを確認してください。必要に応じて、この手順を使用してクラスタ ID を更新することができます。
Step 5	プレゼンスの更新のスロットル率の設定（146 ページ）	オプション。メッセージで 1秒当たりに Cisco XCP Router に送信されるアベイラビリティ（プレゼンス）変更レートを設定できます。この設定で、IM and Presence Service が設定値に合わせてアベイラビリティ（プレゼンス）変更レートを調整する際の過負荷防止に役立ちます。
Step 6	スタティック ルートの設定（147ページ）	スタティック ルートを設定する際は、このタスクを実行します。

ルーティング通信方法の設定

IM and Presence Service がクラスタ ノード間のルータ接続を確立するために使用するルーティング方法は、ルーティングの通信タイプによって決定されます。単一ノードの IM and Presence Service 展開の場合は、ルーティング通信タイプをデフォルト設定のままにすることを推奨します。

⚠

注意　クラスタ設定を完了し、IM and Presence Service 展開へのユーザ トラフィックの受け入れを開始する前に、ルーティング通信タイプを設定する必要があります。

始める前に

MDNS ルーティングを使用する場合は、IOS ネットワーク全体で MDNS を有効にする必要があります。

手順

Step 1　IM and Presence データベース パブリッシャ ノードで、Cisco Unified CM IM and Presence Administration にログインします。

Step 2　**[System（システム）] > [Service Parameters（サービス パラメータ）]** を選択します。

Step 3　**サーバ** ドロップダウン リスト ボックスから、IM and Presence Service ノードを選択します。

Step 4　**サービス** ドロップダウン リストから**Cisco XCP Router**を選択します。

Step 5　**XCP Router グローバル設定（Clusterwide）**の下でルーティング タイプに **ルーティング通信タイプ** サービス パラメータを選択します。

- **マルチキャスト DNS（MDNS）**：クラスタのノードが同じマルチキャスト ドメインにある場合は、マルチキャスト DNS 通信を選択します。
- **ルータ間（自動）**：クラスタのノードが同じマルチキャスト ドメイン内にない場合、ルータ間通信を選択します。これがデフォルト設定です。

  （注）　ルータ間接続を使用する場合の展開では、IM and Presence Service が XCP ルート ファブリックを確立する間に、パフォーマンスのオーバーヘッドが追加で発生します。

Step 6　**[保存（Save）]** をクリックします。

次のタスク

この設定を編集した場合は、以下が必要となります。 Cisco XCP ルータの再起動 （144 ページ）

Cisco XCP ルータの再起動

ルーティングの通信タイプを編集した場合は、Cisco XCP ルータ サービスを再起動する必要があります。

始める前に

ルーティング通信方法の設定 （143 ページ）

手順

Step 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-ネットワークサービス（Control Center - Network Services）]** を選択します。

Step 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。

Step 3 **IM and Presence Services** エリアで、**Cisco XCP Router**を選択します。

Step 4 [再起動（Restart）] をクリックします。

次のタスク

ルータ間のルーティングが設定されている場合は、「セキュアなルータ間コミュニケーションの設定 （145 ページ）」に進みます。

MDNS ルーティングが設定されている場合は、「クラスタ ID の設定 （146 ページ）」に進みます。

セキュアなルータ間コミュニケーションの設定

ルーター間通信が設定されている場合は、このオプション手順を使えば、同じクラスタ内または異なるクラスタ内の XMPP ルータ間でセキュア TLS 接続を使用することができます。IM and Presence Service は XMPP 証明書を XMPP 信頼証明書として自動的にクラスタ内またはクラスタ間で複製します。

（注） このオプションは、パフォーマンスが低下する場合があります。IM and Presence サービスがセキュリティ保護されていないネットワーク上で実行されている場合にのみ有効にしてください。

手順

Step 1 Cisco Unified CM IM and Presence 管理で、**システム** > **セキュリティ** > **設定**を選択します。

Step 2 **XMPP ルータ ツールータ セキュア モードの有効化** のチェック ボックスをオンにします。

Step 3 [保存（Save）] をクリックします。

次のタスク

プレゼンスの更新のスロットル率の設定 （146 ページ）

クラスタ ID の設定

MDNS ルーティングを使用する場合は、**クラスタ ID** がクラスタ内のすべてのノードで共有されていること、また、その値がクラスタ内で一意であることを確認してください。必要に応じて、この手順を使用して**クラスタ ID**を更新することができます。

（注） インストール時に、システムはデフォルトの固有の**クラスタ ID**を IM and Presence Service クラスタに割り当てます。変更の必要がある場合以外は、デフォルトの設定値をそのままにしておくことを推奨します。

手順

Step 1 IM and Presence データベース パブリッシャ ノードで、Cisco Unified CM IM and Presence 管理にログインします。

Step 2 **プレゼンス** > **設定** > **標準設定**を選択します。

Step 3 **クラスタ ID** フィールドの値を確認します。ID を編集する必要がある場合は、新しい値を入力します。

IM and Presence サービスは、クラスタ ID 値でのアンダースコア文字（_）を許可しません。クラスタ ID 値にこの文字が含まれていないことを確認します。

Step 4 **[保存（Save）]** をクリックします。
クラスタ IDを編集した場合は、新しい設定がすべてのクラスタ ノードに複製されます。

次のタスク

プレゼンスの更新のスロットル率の設定 （146 ページ）

プレゼンスの更新のスロットル率の設定

このオプショナルの設定手順で、メッセージで1秒当たりにCisco XCP Routerに送信されるアベイラビリティ（プレゼンス）変更レートを設定します。この設定で、IM and Presence Service が設定値に合わせてアベイラビリティ（プレゼンス）変更レートを戻す際の過負荷防止に役立ちます。

手順

Step 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。

Step 2 [サーバ（Server）] ドロップダウン リスト ボックスから、[IM and Presence サービス（IM and Presence Service）] ノードを選択します。

Step 3 **サービス** ドロップダウン リスト ボックスから、**Cisco プレゼンス エンジン**を選択します。

Step 4 **Clusterwide パラメータ** セクションで、**プレゼンス変更スロットル率** サービス パラメータを編集します。有効な範囲は 10 ~ 100 で、デフォルト設定は 50 です。

Step 5 **[保存（Save）]** をクリックします。

次のタスク

フェデレーション接続に SIP スタティックルートを設定する必要がある場合は、「スタティックルートの設定 （147 ページ）」に進みます。

スタティック ルートの設定

手順

	コマンドまたはアクション	目的
Step 1	SIP プロキシ サーバ構成の設定 （147 ページ）	SIP プロキシ サーバ構成の設定WAN 展開では、IM and Presence Service で TCP メソッドイベントのルーティングを有効にすることを推奨します。
Step 2	IM and Presence Service のルート組み込みテンプレートの設定 （148 ページ）	スタティック ルートに埋め込みワイルドカードが含まれている場合は、ルート埋め込みテンプレートを設定する必要があります。
Step 3	IM and Presence Service のスタティック ルートの設定 （149 ページ）	スタティック ルートの構成を設定します。

SIP プロキシ サーバ構成の設定

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**プレゼンス** > **ルーティング** > **設定**を選択します。

Step 2 [Method/Event Routing Status（メソッド/イベント ルーティングのステータス）] で **[On（オン）]** を選択します。WAN 展開では、IM and Presence Service で TCP メソッドイベントのルーティングを設定することを推奨します。

Step 3 [優先プロキシ サーバ（Preferred Proxy Server）] で **[デフォルト SIP プロキシ TCP リスナー（Default SIP Proxy TCP Listener）]** を選択します。

Step 4 [保存（Save）] をクリックします。

IM and Presence Service のルート組み込みテンプレートの設定

スタティック ルートに埋め込みワイルドカードが含まれている場合は、ルート埋め込みテンプレートを設定する必要があります。

手順

Step 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。

Step 2 **サーバ** ドロップダウン リストから IM and Presence Service サーバを選択します。

Step 3 **サービス** ドロップダウンで、**Cisco SIP プロキシ**を選択します。

Step 4 **ルーティング パラメータ**（**Clusterwide**）の下の**RouteEmbedTemplate** フィールドに、使用するテンプレートを入力します。最大 5 つのテンプレートを定義することができます。ただし、単一のルート組み込みテンプレートに定義できるスタティック ルートの数に制限はありません。

Step 5 [保存（Save）] をクリックします。

次のタスク

IM and Presence Service のスタティック ルートの設定 （149 ページ）

ルート組み込みテンプレート

組み込みのワイルドカードを含む任意のスタティック ルート パターンのルート組み込みテンプレートを定義する必要があります。ルート組み込みテンプレートには、組み込みのワイルドカードの先頭の数字、数字の長さ、および場所に関する情報が含まれます。ルート組み込みテンプレートを定義する前に、次のサンプル テンプレートを考慮してください。

ルート組み込みテンプレートを定義する際、「.」に続く文字は、スタティック ルートの実際のテレフォニーの数字と一致しなければなりません。以下のルート組み込みテンプレートの例では、これらの文字を「x」で表しています。

サンプル ルート組み込みテンプレート A

ルート組み込みテンプレート：`74..78xxxxx*`

このテンプレートでは、IM and Presence Service は、組み込みのワイルドカードでスタティック ルートの次のセットを有効にします。

表 *13*：組み込みワイルドカードで設定したスタティック ルート - テンプレート *A*

宛先パターン（**Destination Pattern**）	ネクスト ホップ宛先
74..7812345*	1.2.3.4:5060
74..7867890*	5.6.7.8.9:5060
74..7811993*	10.10.11.37:5060

このテンプレートでは、IM and Presence Service は次のスタティック ルート エントリを有効にしません。

- 73..7812345*（最初の文字列がテンプレートで定義されている「74」ではない）
- 74..781*（宛先パターンの数字の長さがテンプレートと一致しない）
- 74…7812345*（ワイルドカードの数がテンプレートと一致しない）

サンプル ルート組み込みテンプレート B

ルート組み込みテンプレート：`471….xx*`

このテンプレートでは、IM and Presence Service は、組み込みのワイルドカードでスタティック ルートの次のセットを有効にします。

表 *14 :* 組み込みワイルドカードで設定したスタティック ルート - テンプレート *B*

宛先パターン（Destination Pattern）	ネクスト ホップ宛先
471….34*	20.20.21.22
471…55*	21.21.55.79

このテンプレートでは、IM and Presence Service は次のスタティック ルート エントリを有効にしません。

- 47…344*（最初の文字列がテンプレートで定義されている「471」ではない）
- 471…4*（文字列の長さがテンプレートと一致しない）
- 471.450*（ワイルドカードの数がテンプレートと一致しない）

IM and Presence Service のスタティック ルートの設定

スタティック ルートを設定するには、次の手順を使用します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**ルーティング** > **スタティック ルート**を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 **接続先パターン**で、ルート パターンを入力します。

Step 4 **ネクスト ホップ** フィールドに以下のホップの IP アドレスを入力します。

Step 5 **ネクストホップのポート**で、ネクストホップのサーバの接続先ポートを入力します。デフォルトのポートは 5060 です。

Step 6 **ルート タイプ** ドロップダウンで、ルート タイプに**ユーザ** あるいは **ドメイン**を選択します。

Step 7 **プロトコル タイプ** ドロップダウン リスト ボックスで、スタティック ルートのプロトコルに、**TCP**、**UDP**、あるいは**TLS**のいずれかのプロトコルを選択します。

Step 8 **スタティック ルート設定** ウィンドウで、残りのフィールド入力を完了します。

Step 9 [保存（Save）] をクリックします。

スタティック ルート パラメータの設定

次の表は、IM and Presence Service で設定できるスタティック ルート パラメータ設定の一覧です。

表 15 : IM and Presence Service のスタティック ルート パラメータ設定

フィールド	説明
宛先パターン（Destination Pattern）	着信番号のパターンを 255 文字以内で指定します。 SIP プロキシでは、100 本のスタティック ルートにだけ同じルート パターンを割り当てることができます。この制限を超えた場合、IM and Presence Service はエラーをログに記録します。 ワイルドカードの使用方法 単一文字のワイルドカードとして「.」を、複数文字のワイルドカードとして「*」を使用することができます。 IM and Presence Service は、スタティック ルートにおける組み込みのワイルドカード文字である「.」をサポートします。ただし、組み込みのワイルドカードを含むスタティック ルートのルート組み込みテンプレートを定義する必要があります。組み込みのワイルドカードを含むスタティック ルートは、ルート組み込みテンプレートの少なくとも 1 つと一致する必要があります。ルート組み込みテンプレートの定義については、ルート組み込みテンプレートのトピック（次の「関連トピック」内）を参照してください。 電話機の場合： • ドットはパターンの末尾に置くことも、パターンに組み込むこともできます。パターンにドットを組み込む場合は、パターンに一致するルート組み込みテンプレートを作成する必要があります。 • アスタリスクは、パターンの最後だけに使用できます。 IP アドレスおよびホスト名の場合： • アスタリスクはホスト名の一部として使用できます。 • ドットはホスト名のリテラル値の役割を果たします。 エスケープ文字とアスタリスクの連続（*）はリテラル * と一致し、任意の場所で使用できます。
説明	特定のスタティック ルートの説明を 255 文字以内で指定します。

フィールド	説明
ネクスト ホップ	着信先（ネクスト ホップ）のドメイン名または IP アドレスを指定し、完全修飾ドメイン名（FQDN）またはドット付き IP アドレスのいずれかにすることができます。 IM and Presence Service では、DNS SRV ベースのコール ルーティングをサポートしています。DNS SRV をスタティック ルート用のネクスト ホップとして指定する場合は、このパラメータを該当する DNS SRV の名前に設定します。
ネクスト ホップ ポート（Next Hop Port）	着信先（ネクストホップ）のポート番号を指定します。デフォルトのポートは 5060 です。 IM and Presence Service では、DNS SRV ベースのコール ルーティングをサポートしています。DNS SRV をスタティック ルート用のネクスト ホップとして指定する場合は、このパラメータを 0 に設定します。
ルート タイプ	ルート タイプを指定します（[ユーザ（User）] または [ドメイン（Domain）]）。デフォルト値は [ユーザ（User）] です。 たとえば、SIP URI sip:19194762030@myhost.com 要求では、ユーザ部分は 19194762030 で、ホスト部分は myhost.com です。ルート タイプとして [ユーザ] を選択すると、IM and Presence Service は SIP トラフィックをルーティングするためにユーザ部分の値「19194762030」を使用します。ルート タイプとして[ドメイン] を選択すると、IM and Presence Service は SIP トラフィックをルーティングするために「myhost.com」を使用します。
プロトコルタイプ	このルートのプロトコル タイプ（TCP、UDP、または TLS）を指定します。デフォルト値は TCP です。
優先度	このルートのプライオリティ レベルを指定します。値が小さいほど、プライオリティが高くなります。デフォルト値は 1 です。 値の範囲：1 ～ 65535

フィールド	説明
ウェイト（Weight）	ルートの重み付けを指定します。このパラメータは、複数のルートのプライオリティが同じ場合に限り使用します。値が大きいほど、ルートのプライオリティが高くなります。 値の範囲：1 ～ 65535 **例**：次のプライオリティと重み付けが関連付けられた 3 本のルートがあるとします。 • 1、20 • 1、10 • 2、50 この例では、スタティック ルートが適切な順序で表示されています。プライオリティルートは、最低値のプライオリティ（値1）が基準となります。2 つのルートが同じプライオリティを共有している場合、値の高いほうの重量パラメータによってプライオリティ ルートが決定します。この例では、IM and Presence Service はプライオリティ値として 1 が設定されている両方のルートに SIP トラフィックを送信し、重み付けに従ってトラフィックを分散させます。重み付けが 20 のルートは、重み付けが 10 のルートの 2 倍のトラフィックを受信します。この例では、IM and Presence Service はプライオリティ 1 の両方のルートを試み、両方が失敗した場合だけプライオリティ 2 のルートを使用しようとします。
固有性の低いルートを許可（Allow Less-Specific Route）	固有性の低いルートを許可することを示します。デフォルト設定はオンです。
In Service（サービス中）	ルートをアウト オブ サービスにするかどうかを指定します。ルートをアウト オブ サービスにするかどうかを指定します。
[ルートのブロック（Block Route）] チェックボックス	オンにすると、スタティック ルートがブロックされます。デフォルト設定は、ブロック解除です。

第 12 章

証明書の設定

証明書の概要

アイデンティティを保護し、IM and Presence Serviceと別のシステム間の信頼関係を構築するために証明書が使用されます。証明書を使用すると、IM and Presence Service を Cisco Jabber クライアント、または任意の外部サーバに接続することが可能です。証明書がなければ、不正なDNSサーバーが使用されていないか、または別のサーバにルーティングされていないかを判断することはできません。

IM and Presence Service が使用できる証明書には、以下の 2 つの主要なクラスがあります。

- 自己署名証明書：自己署名証明書は、証明書を発行したサーバと同じサーバによって署名されます。企業内では、セキュアでないネットワークに接続している接続がない場合は、自己署名付きの証明書を使用して、別の内部システムに接続することができます。たとえば、IM and Presence Service は、Cisco Unified Communications Manager への内部接続に、自己署名証明書を生成する場合があります。

- CA 署名付き証明書：CA 署名付き証明書は、サードパーティ認証局 (CA) によって署名された証明書です。CA署名付き証明書は、サーバあるいはサービス証明書の有効性を制御するパブリック CA（Verisign、Entrust、または Digicert）あるいはサーバ（Windows 2003、Linux、Unix、IOSなど）によって署名されている場合があります。CA署名付き証明書は、自己署名証明書よりも安全であり、通常、WAN接続に使用されます。たとえば、別の企業またはWAN接続を使用したクラスタ間ピア構成では、外部システムとの信頼関係を構築するために CA 署名付きの証明書が必要となります。

CA 署名付き証明書は、自己署名証明書よりも安全です。通常、自己署名付き証明書は内部接続では十分であると見なされますが、パブリック インターネット経由あるいは WAN 経由で接続する場合は、CA 署名付き証明書を使用する必要があります。

マルチサーバ証明書

IM and Presence Service は、いくつかのシステム サービスのマルチサーバ SAN 証明書もサポートしています。複数のサーバ証明書の証明書署名要求（CSR）を生成すると、証明書がアップロードされる際、結果として得られるマルチサーバ証明書とその証明書のチェーンは、すべてのクラスタ ノードに自動的に配布されます。

IM and Presence Services の証明書タイプ

IM and Presence Service 内のさまざまなシステム コンポーネントには、さまざまな種類の証明書が必要です。以下のテーブルでは、IM and Presence Service のクライアントおよびサービスで必要とされるさまざまな証明書について説明します。

（注） 証明書名が -ECDSA で終わる場合、その 証明書/キー タイプは楕円曲線（EC）です。それ以外の場合は、RSA です。

表 *16 :* 証明書タイプおよびサービス

証明書タイプ	サービス	証明書信頼ストア	マルチサーバ サポート	注記
tomcat tomcat-ECDSA	Cisco Client Profile Agent Cisco AXL Web Service Cisco Tomcat	tomcat- trust	はい	IM and Presence Service のクライアント認証の一部として Cisco Jabber クライアントに提示されます。 Cisco Unified CM IM and Presence 管理ユーザインターフェイスを移動するときに、Webブラウザに表示されます。 関連する信頼ストアを使用し、ユーザのクレデンシャルを認証するために、IM and Presence Service が確立した設定済みの LDAP サーバとの 接続を確認します。
IPSec		ipsec-trust	非対応	IPSec ポリシーが有効になっている場合に使用します。

証明書タイプ	サービス	証明書信頼ストア	マルチサーバ サポート	注記
CUP cup-ECDSA	Cisco SIP Proxy Cisco Presence Engine	cup-trust	非対応	Expressway-C に証明書を提示して、SIP フェデレーションユーザ用の IM and Presence を取得します。IM and Presence プロキシは、クライアントとサーバの両方として動作します。 プレゼンスエンジンは、これらの証明書を Exchange/Office 365 との通信に使用してカレンダープレゼンスを取得します。プレゼンスエンジンは、クライアントとしてのみ動作します。
cup-xmpp cup-xmpp-ECDSA	Cisco XCP Connection Manager Cisco XCP Web Connection Manager Cisco XCP Directory サービス Cisco XCP Router サービス	cup-xmpp-trust	はい	XMPP セッションの作成中に、Cisco Jabber クライアント、サードパーティ製 XMPP クライアント、または CAXL ベースのアプリケーションに提示されます。 関連する信頼ストアを使用して、サードパーティ製 XMPP クライアントの LDAP 検索操作を実行中に Cisco XCP Directory サービスが確立した接続を確認します。 ルーティング通信タイプがルータ間に設定されている場合に、IM and Presence Service サーバ間にセキュアな接続を確立するときに Cisco XCP Router によって関連する信頼ストアが使用されます。
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Cisco XCP XMPP Federation Connection Manager	cup-xmpp-trust	はい	外部フェデレーション XMPP への接続時に XMPP ドメイン間フェデレーションを行うために提示されます。

証明書の前提条件

Cisco Unified Communications Manager で次の項目を設定します。

- IM and Presence サービスの SIP トランク セキュリティ プロファイルを設定します。
- IM and Presence Service の SIP トランクを設定します。
  - SIP トランクにセキュリティ プロファイルを関連付けます。

- IM and Presence Service 証明書のサブジェクト共通名（CN）を SIP トランクに設定します。

Cisco Unified Communications Manager との証明書交換

これらのタスクを完了して、Cisco Unified Communications Manager と交換を行います。

（注） Cisco Unified Communications Manager と IM and Presence Service の間の証明書の交換は、インストールの過程で自動的に処理されます。ただし、証明書交換を手動で行う必要がある場合は、このタスクを実行してください。

手順

	コマンドまたはアクション	目的
Step 1	IM and Presence サービスへの Cisco Unified Communications Manager 証明書のインポート（156 ページ）	IM and Presence サービスに Cisco Unified Communications Manager 証明書をインポートします。
Step 2	IM and Presence サービスからの証明書のダウンロード（157 ページ）	IM and Presence Service から証明書をダウンロードします。証明書は Cisco Unified Communications Manager にインポートする必要があります。
Step 3	IM and Presence への Cisco Unified Communications Manager 証明書のインポート（158 ページ）	証明書の交換を完了するには、IM and Presence Service の証明書を Cisco Unified Communications Manager の Callmanager-trust にインポートします。

IM and Presence サービスへの Cisco Unified Communications Manager 証明書のインポート

この手順で、IM and Presence Service に Cisco Unified Communications Manager 証明書をインポートします。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**システム** > **セキュリティ** > **証明書インポート ツール**を選択します。

Step 2 **[Certificate Trust Store（証明書信頼ストア）]** メニューから **[IM and Presence（IM/P）Service Trust（IM and Presence（IM/P）サービス信頼）]** を選択します。

Step 3 Cisco Unified Communications Manager ノードの IP アドレス、ホスト名、または FQDN を入力します。

Step 4 Cisco Unified Communications Manager ノードと通信するポート番号を入力します。

Step 5 [送信（Submit）] をクリックします。

（注） 証明書インポート ツールのインポート操作が完了すると、Cisco Unified Communications Manager に正常に接続したかどうか、また、Cisco Unified Communications Manager から証明書が正常にダウンロードされたかどうかが報告されます。証明書インポート ツールで障害が報告された場合、推奨処置についてはオンライン ヘルプを参照してください。**[Cisco Unified IM and Presence OS の管理（Cisco Unified IM and Presence OS Administration）] > [セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択して、手動で証明書をインポートすることもできます。

（注） ネゴシエートされる TLS 暗号方式に応じて、証明書インポート ツールにより、RSA ベースの証明書または ECDSA ベースの証明書のいずれかがダウンロードされます。

Step 6 Cisco SIP Proxy サービスを再起動します。

a) Cisco Unified IM and Presence Serviceabilityから、IM and Presence Service に **ツール** > **コントロール センター - 機能サービス**を選択します。

b) **サーバ** ドロップダウン リスト ボックスで、IM and Presence Service クラスタ ノードを選択し、**移動**をクリックします。

c) **Cisco SIP プロキシ**を選択して、**再起動**をクリックします。

次のタスク

IM and Presence サービスからの証明書のダウンロード （157 ページ）

IM and Presence サービスからの証明書のダウンロード

この手順で、IM and Presence Service から証明書をダウンロードします。証明書を Cisco Unified Communications Manager にインポートする必要があります。

手順

Step 1 **Cisco Unified IM and Presence OS 管理**から、IM and Presence Service で**セキュリティ** > 証明書管理を選択します。

Step 2 [検索（Find）] をクリックします。

Step 3 `cup.pem` ファイルを選択します。

（注） `cup-ECDSA`は、使用可能なオプションでもあります。

Step 4 [ダウンロード] をクリックして、ローカル コンピュータにファイルを保存します。

ヒント IM and Presence サービスが表示する cup.csr ファイルへのアクセスに関するすべてのエラーを無視してください。Cisco Unified Communications Manager と交換する証明書に CA（認証局）が署名する必要はありません。

次のタスク

IM and Presence への Cisco Unified Communications Manager 証明書のインポート （158 ページ）

IM and Presence への Cisco Unified Communications Manager 証明書のインポート

証明書の交換を完了するには、IM and Presence Service の証明書を Cisco Unified Communications Manager の Callmanager-trust にインポートします。

始める前に

IM and Presence サービスからの証明書のダウンロード （157 ページ）

手順

Step 1 Cisco Unified OS の管理にログインします。

Step 2 **セキュリティ** > **証明書管理**を選択する

Step 3 [証明書のアップロード（Upload Certificate）] をクリックします。

Step 4 [証明書名]メニューから **Callmanager-trust** を選択します。

Step 5 IM and Presence から以前にダウンロードした証明書を**参照し**、選択します。

Step 6 [ファイルのアップロード（Upload File）] をクリックします。

Step 7 Cisco CallManager サービスの再起動:

a) Cisco Unified 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）]** の順に選択します。

b) **サーバ** ドロップダウン リスト ボックスから、Cisco Unified Communications Manager ノードを選択して、**移動**をクリックします。

c) **Cisco CallManager** サービスを選択し、**再起動**をクリックします。

IM and Presence Service での証明機関 (CA) のインストール

IM and Presence Service でサードパーティ認証局 (CA) によって署名された証明書を使用するには、まず、IM and Presence Service で信頼できるルート証明書チェーンをインストールする必要があります。

手順

	コマンドまたはアクション	目的
Step 1	CA ルート証明書チェーンのアップロード（159 ページ）	この手段で、サードパーティ認証局から IM and Presence Service に CA ルート証明書チェーンをアップロードします。
Step 2	Cisco Intercluster Sync Agent サービスの再起動（160 ページ）	証明書のアップロードが完了したら、Cisco Intercluster Sync Agent サービスを再起動します。
Step 3	他のクラスタに CA 証明書が同期されていることの確認（160 ページ）	CA 証明書チェーンがすべてのピア クラスタに複製されていることを確認します。

CA ルート証明書チェーンのアップロード

この手順を使用して、署名認証局 (CA) から IM and Presence データベースのパブリッシャーノードに証明書チェーンをアップロードします。このチェーンは、チェーン内の複数の証明書で構成されており、各証明書が後続の証明書に署名している場合があります。

- ルート証明書 > 中間 1 証明書 > 中間 2 証明書

手順

Step 1 IM and Presence データベース パブリッシャ ノードで、Cisco Unified CM IM and Presence OS 管理にログインします。

Step 2 **[Security（セキュリティ）] > [Certificate Management（証明書管理）]** を選択します。

Step 3 [Upload Certificate/Certificate chain] をクリックします。

Step 4 **証明書名** ドロップダウン リストから、以下のいずれかを選択します。

- CA 署名付きの tomact 証明書をアップロードする場合は、**tomcat-trust**を選択してください。
- CA が署名した cup-xmpp 証明書あるいは CA で署名されたcup-xmpp-s2s をアップロードする場合は、**cup-xmpp-s2s**を選択します。

Step 5 署名付き証明書の**説明**を入力します。

Step 6 **[Browse（参照）]** をクリックしてルート証明書のファイルを見つけます。

Step 7 **ファイルのアップロードをクリック**をクリックします。

Step 8 同じ方法で、**証明書および証明書チェーンのアップロード** ウィンドウを使用して、それぞれの中間証明書をアップロードします。それぞれの中間証明書について、チェーンで先行する証明書名を入力する必要があります。

次のタスク

Cisco Intercluster Sync Agent サービスの再起動 （160 ページ）

Cisco Intercluster Sync Agent サービスの再起動

IM and Presence データベース パブリッシャ ノードにルートおよび中間証明書をアップロードしたら、そのノードで Cisco Intercluster Sync Agent サービスを再起動する必要があります。この再起動で、ただちに CA 証明書が他のすべてのクラスタで同期されます。

手順

Step 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-ネットワークサービス（Control Center - Network Services）]** を選択します。

Step 2 **サーバ** ドロップダウン リスト ボックスで、証明書をインポートした IM and Presence Service ノードを選択して、**移動**をクリックします。

（注） CLI（コマンドラインインターフェイス）で、`utils service restart Cisco Intercluster Sync Agent` を実行して Cisco Intercluster Sync Agent サービスを再起動することもできます。

Step 3 **Cisco Intercluster Sync Agent** サービスを選択して、**再起動**をクリックします。

次のタスク

クラスタ間同期の確認 （164 ページ）

他のクラスタに CA 証明書が同期されていることの確認

Cisco Intercluster Sync Agent サービスが再起動した後、CA 証明書が他のクラスタに正しく同期されたことを確認する必要があります。他の IM and Presence データベース パブリッシャの各ノードで、次の手順を実行します。

（注） この手順の情報は、-ECDSA で終わる証明書にも適用されます。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、診断 > **システムのトラブルシューティング**を選択します。

Step 2 **[クラスタ間トラブルシュータ（Inter-clustering Troubleshooter）]** で、**[各 TLS 対応クラスタ間ピアが正常にセキュリティ証明書を交換しました（Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates）]** テストを検索し、テストに合格していることを確認します。

Step 3 テストでエラーが表示される場合は、クラスタ間ピアの IP アドレスを記録します。この IP アドレスは、CA 証明書をアップロードしたクラスタを参照している必要があります。次のステップを続行し、問題を解決します。

Step 4 **[プレゼンス（Presence）]**>**[クラスタ間（Inter-Clustering）]** を選択し、[システム トラブルシュータ（System Troubleshooter）] ページで識別したクラスタ間ピアに関連付けられているリンクをクリックします。

Step 5 **[強制手動同期（Force Manual Sync）]** をクリックします。

Step 6 クラスタ間ピア ステータス パネルの自動リフレッシュには、60 秒かかります。

Step 7 **[証明書のステータス（Certificate Status）]** フィールドに「セキュアな接続です（Connection is secure）」が表示されていることを確認します。

Step 8 [Certificate Status（証明書のステータス）] フィールドに「Connection is secure（セキュアな接続です）」が表示されていない場合は、IM and Presence データベース パブリッシャ ノードで Cisco Intercluster Sync Agent サービスを再起動してから、ステップ 5 ～ 7 を繰り返します。

- 管理者 CLI からサービスを再起動するには、utils service restart Cisco Intercluster Sync Agent コマンドを実行します。
- また、Cisco Unified IM and Presence Serviceability の GUI からこのサービスを再起動できます。

Step 9 この時点で **[証明書のステータス（Certificate Status）]** フィールドに「セキュアな接続です（Connection is secure）」が表示されていることを確認します。これは、クラスタ間同期がクラスタ間で正常に確立され、アップロードした CA 証明書がほかのクラスタに同期していることを意味します。

次のタスク

各 IM and Presence Service ノードへ署名付き証明書をアップロードします。

IM and Presence Service への証明書のアップロード

以下のタスクを実行して、IM and Presence Service 用の 証明書をアップロードします。CA 署名付き証明書または自己署名証明書をアップロードすることが可能です。

始める前に

サードパーティ認証局 (CA) によって署名された CA 署名済みの証明書を使用するには、その CA のルート証明書チェーンを既に IM and Presence Service にインストールしている必要があります。詳細は、「IM and Presence Service での証明機関 (CA) のインストール（159 ページ）」を参照してください。

手順

	コマンドまたはアクション	目的
Step 1	証明書のアップロード（Upload Certificates）（163 ページ）	IM and Presence Service に署名付き証明書をアップロードします。
Step 2	Cisco Tomcat サービスの再起動（163 ページ）	（tomcat 証明書のみ）。Cisco Tomcat サービスを再起動します。
Step 3	クラスタ間同期の確認（164 ページ）	（tomcat 証明書のみ）。Cisco Tomcat サービスがクラスタ内の影響を受けるすべてのノードに対して再起動した後、クラスタ間同期が正常に動作していることを確認する必要があります。
Step 4	すべてのノードで Cisco XCP ルータ サービスを再起動します。（165 ページ）	cup-xmpp ストアに証明書をアップロードした場合は、すべてのクラスタ ノード上で Cisco XMP Router を再起動します。
Step 5	Cisco XCP XMPP Federation Connection Manager サービスの再起動（165 ページ）	（XMPP フェデレーションのみ）。XMPP フェデレーション用の cup-xmpp ストアに証明書をアップロードした場合は、Cisco XCPXMPP フェデレーションサービスを再起動します。
Step 6	XMPP フェデレーションのセキュリティ証明書でのワイルドカードの有効化（166 ページ）	（XMPP フェデレーションのみ）。TLS を介して XMPP フェデレーション用の cup-xmpp ストアに証明書をアップロードした場合は、XMPP セキュリティ証明書のワイルドカードを有効にする必要があります。これはグループ チャットに必要です。

証明書のアップロード（Upload Certificates）

各 IM and Presence Service ノードに署名付き証明書をアップロードします。

（注） クラスタに必要なすべての tomcat 証明書に署名し、それらを同時にアップロードすることを推奨します。この方法を使用すると、クラスタ間通信のリカバリに要する時間が短縮されます。

（注） この手順の情報は、`-ECDSA` で終わる証明書にも適用されます。

始める前に

証明書がCAによって署名されている場合は、そのCAのルート証明書チェーンがインストールされている必要があります。でないと、CA 署名証明書が信頼されないものとみなされます。CA 証明書がすべてのクラスタに正しく同期されている場合は、各 IM and Presence Service ノードに適切な署名付き 証明書をアップロードできます。

手順

Step 1 **Cisco Unified IM and Presence OS 管理**で、**セキュリティ** > **証明書管理**を選択します。

Step 2 [Upload Certificate/Certificate chain] をクリックします。

Step 3 **証明書の目的**を選択します。たとえば、**tomcat**とします。

Step 4 署名付き証明書の説明を入力します。

Step 5 アップロードするファイルを検索するには、**[参照（Browse）]** をクリックします。

Step 6 [ファイルのアップロード] をクリックします。

Step 7 各 IM and Presence Service ノードで繰り返します。

次のタスク

Cisco Tomcat サービスを再起動します。

Cisco Tomcat サービスの再起動

各 IM and Presence サービス ノードに tomcat 証明書をアップロードしたら、各ノードで Cisco Tomcat サービスを再起動する必要があります。

手順

Step 1 管理 CLI にログインします。

Step 2 次のコマンドを実行します。`utils service restart Cisco Tomcat`。

Step 3 各ノードで繰り返します。

次のタスク

クラスタ間同期が正常に動作していることを確認します。

クラスタ間同期の確認

Cisco Tomcat サービスがクラスタ内の影響を受けるすべてのノードに対して再起動した後、クラスタ間同期が正常に動作していることを確認する必要があります。他のクラスタの各 IM and Presence データベース パブリッシャ ノードで次の手順を実行します。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**診断** > **システムのトラブルシューティング**を選択します。

Step 2 **[クラスタ間トラブルシュータ（Inter-clustering Troubleshooter）]** で、**[各 TLS 対応クラスタ間ピアがセキュリティ証明書を正常に交換していることを確認する（Verify that each TLS-enabled inter-cluster peer has successfully exchanged security certificates）]** テストを検索し、テストに合格していることを確認します。

Step 3 テストでエラーが表示される場合は、クラスタ間ピアの IP アドレスを記録します。この IP アドレスは、CA 証明書をアップロードしたクラスタを参照している必要があります。次のステップを続行し、問題を解決します。

Step 4 **プレゼンス** > **クラスタ間** を選択し、[システムのトラブルシューティング] ページで、識別したクラスタ間ピアに関連付けられているリンクをクリックします。

Step 5 **[強制手動同期（Force Manual Sync）]** をクリックします。

Step 6 **[ピアの Tomcat 証明書も再同期します（Also resync peer's Tomcat certificates）]** チェックボックスをオンにし、**[OK]** をクリックします。

Step 7 クラスタ間ピア ステータス パネルの自動リフレッシュには、60 秒かかります。

Step 8 **[証明書のステータス（Certificate Status）]** フィールドに「セキュアな接続です（Connection is secure）」が表示されていることを確認します。

Step 9 **[証明書のステータス（Certificate Status）]** フィールドに「セキュアな接続です（Connection is secure）」が表示されていない場合は、IM and Presence データベース パブリッシャ ノードで Cisco Intercluster Sync Agent サービスを再起動してから、ステップ 5 ～ 8 を繰り返します。

- 管理者 CLI からサービスを再起動するには、[utils service restart Cisco Intercluster Sync Agent] コマンドを実行します。

- また、Cisco Unified IM and Presence Serviceability の GUI からこのサービスを再起動できます。

Step 10 この時点で [Certificate Status（証明書のステータス）] フィールドに「Connection is secure（セキュアな接続です）」が表示されていることを確認します。これは、クラスタ間同期が、このクラスタと、証明書をアップロードしたクラスタの間で再確立されていることを意味します。

すべてのノードで Cisco XCP ルータ サービスを再起動します。

各 IM and Presence Service ノードに cup-xmpp の証明書や cup-xmpp-ECDSA の証明書をアップロードしたら、各ノードで Cisco XCP Router サービスを再起動する必要があります。

（注） また、Cisco Unified IM and Presence Serviceability GUI から Cisco XCP Router サービス を再起動できます。

手順

Step 1 管理 CLI にログインします。

Step 2 次のコマンドを実行します。[utils service restart Cisco XCP Router]

Step 3 各ノードで繰り返します。

Cisco XCP XMPP Federation Connection Manager サービスの再起動

各 IM and Presence サービス のフェデレーション ノードに cup-xmpp-s2s の証明書や cup-xmpp-s2s-ECDSA の証明書をアップロードしたら、各フェデレーション ノードの Cisco XCP XMPP Federation Connection Manager サービスを再起動する必要があります。

手順

Step 1 管理 CLI にログインします。

Step 2 次のコマンドを実行します。[utils service restart Cisco XCP XMPP Federation Connection Manager]

Step 3 各フェデレーション ノードで繰り返します。

XMPP フェデレーションのセキュリティ証明書でのワイルドカードの有効化

XMPP フェデレーションのパートナー間での TLS を介してのグループ チャットをサポートするには、XMPP セキュリティ証明書に対するワイルドカードを有効にする必要があります。

デフォルトでは、XMPP フェデレーション セキュリティ証明書の `cup-xmpp-s2s` および `cup-xmpp-s2s-ECDSA` には IM and Presence Service 展開によってホストされるすべてのドメインが含まれます。これらは、証明書内のサブジェクト代替名（SAN）エントリとして追加されます。同じ証明書内のホストされているすべてのドメインにワイルドカードを指定する必要があります。そのため、「example.com」の SAN エントリの代わりに、XMPP セキュリティ証明書には「*.example.com」の SAN エントリが含まれている必要があります。グループ チャットのサーバ エイリアスは、IM and Presence Service システムでホストされているいずれかのドメインのサブドメインであるため、ワイルドカードが必要です。例：「conference.example.com」。

（注） いずれのノードでも、`cup-xmpp-s2s` または `cup-xmpp-s2s-ECDSA` を表示するには、**Cisco Unified IM and Presence OS 管理** > **セキュリティ** > **証明書管理** を選択して、**cup-xmpp-s2s** または **cup-xmpp-s2s-ECDSA** のリンクをクリックします。

手順

Step 1 **[システム（System）]** > **[セキュリティの設定（Security Settings）]** を選択します。

Step 2 [XMPP フェデレーション セキュリティ証明書でのワイルドカードの有効化（Enable Wildcards in XMPP Federation Security Certificates）] をオンにします。

Step 3 [保存（Save）] をクリックします。

次のタスク

Cisco XMPP Federation Connection Manager サービスが実行しており、XMPP フェデレーションが有効になっているクラスタ内のすべてのノードで XMPP フェデレーション セキュリティ証明書を生成する必要があります。このセキュリティ設定は、すべての IM and Presence Service クラスタで有効にし、TLS を介しての XMPP フェデレーションをサポートする必要があります。

CSR を作成する

この手順で、証明書署名要求（CSR）を生成します。CSR は、サードパーティ CA に送信して、CA が署名した証明書を提供してもらう必要があります。

手順

Step 1 [Cisco Unified OS Administration] から **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

Step 2 **CSRの生成** ボタンをクリックします。**証明書署名要求の生成** のポップアップ画面が表示されます。

Step 3 **証明書の目的** ドロップダウンから、生成する証明書のタイプを選択します。

Step 4 **配布** ドロップダウンから、IM and Presence サーバを選択します。マルチサーバ証明書の場合は、**マルチサーバ**を選択します。

Step 5 **キーの長さ**と**ハッシュ アルゴリズム**を入力します。

Step 6 残りのすべてのフィールドの入力を完了して、**生成**をクリックします。

Step 7 CSR をローカル コンピュータにダウンロードします。

a) [CSR のダウンロード（Download CSR）] をクリックします。
b) [証明書の用途（Certificate Purpose）] ドロップダウン リストで、証明書名を選択します。
c) **CSR のダウンロード**

次のタスク

CSR をサードパーティ認証局に送信して、CA 署名付き証明書を発行してもらいます。

証明書署名要求のキー用途拡張

次の表には、Unified Communications Manager と IM and Presence Service の CA 証明書の証明書署名要求（CSR）のキーの用途拡張が表示されています。

***表 17 : Cisco Unified Communications Manager CSR* キーの用途拡張**

	マルチサーバ	キーの拡張用途			キーの用途				
		サーバ認証 **(1.3.6.1.5.5.7.3.1)**	クライアント認証 **(1.3.6.1.5.5.7.3.2)**	IP セキュリティ末端システム **(1.3.6.1.5.5.7.3.5)**	デジタル署名	鍵の暗号化	データの暗号化	キー証明書署名	鍵共有
CallManager CallManager-ECDSA	Y	Y	Y		Y	N	Y		
CAPF（パブリッシャのみ）	N	Y	N		Y	N		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	N	Y		
信頼検証サービス（TVS）	N	Y	Y		Y	Y	Y		

表 *18 : IM and Presence Service CSR* キーの用途拡張

	マルチサーバ	キーの拡張用途			キーの用途				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント認証 (1.3.6.1.5.5.7.3.2)	IP セキュリティ末端システム (1.3.6.1.5.5.7.3.5)	デジタル署名	鍵の暗号化	データの暗号化	キー証明書署名	鍵共有
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

（注） CA 署名証明書のプロセスの一部として、「データ暗号化」ビットが変更または削除されていないことを確認します。

自己署名証明書の生成

この手順で、事故署名証明書を生成します。

手順

Step 1 [Cisco Unified OS Administration] から **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

Step 2 [自己署名証明書の作成（Generate Self-signed）] をクリックします。**新しい自己署名入りの証明書の生成**のポップアップ画面が表示されます。

Step 3 **証明書の目的** ドロップダウンから、生成する証明書のタイプを選択します。

Step 4 **配布** ドロップダウンで、サーバ名を入力します。

Step 5 適切な**キー長**を選択します。

Step 6 **ハッシュ アルゴリズム**から、暗号化アルゴリズムを選択します。たとえば、SHA256 を選びます。

Step 7 [生成（Generate）] をクリックします。

IM and Presence Service の自己署名信頼証明書の削除

同じクラスタ内のノード間でサービスアビリティ用のクロス ナビゲーションをサポートするために、IM and Presence サービスと Cisco Unified Communications Manager の間の Cisco Tomcat サービス信頼ストアが自動的に同期されます。

元の自己署名入りの信頼証明書を CA 署名付き証明書と置き換えた場合、元の自己署名入りの信頼証明書は、サービストラスト ストアに保持されます。この手段で、IM and Presence Service および Cisco Unified Communications Manager の自己署名証明書を削除することができます。

始める前に

重要 CA 署名付き証明書をついたした場合、指定された IM and Presence Service ノード上で Cisco Intercluster Sync Agent サービスが定期的なクリーンアップ タスクを実行するのを 30 分待機してください。

手順

Step 1 Cisco Unified IM and Presence OS 管理で、**セキュリティ** > **証明書管理**を選択します。

Step 2 [検索（Find）] をクリックします。

[証明書の一覧（Certificate List）] が表示されます。

（注） 証明書の名前は、サービス名と証明書タイプの 2 つの部分で構成されています。たとえば tomcat-trust では、tomcat がサービスで trust が証明書タイプです。

削除できる自己署名付き信頼証明書は、次のとおりです。

- Tomcat および Tomcat-ECDSA：tomcat-trust
- Cup-xmpp および Cup-xmpp-ECDSA：cup-xmpp-trust
- Cup-xmpp-s2s および Cup-xmpp-s2s-ECDSA：cup-xmpp-trust
- カップとカップ-ECDSA: カップトラスト
- Ipsec：ipsec-trust

Step 3 削除する自己署名付き信頼証明書のリンクをクリックします。

重要 サービス信頼ストアに関連付けられているサービスに対して、CA 署名付き証明書がすでに設定されていることを確認します。

新しいウィンドウが表示され、証明書の詳細が示されます。

Step 4 [削除（Delete）] をクリックします。

（注） **削除** ボタンは、削除する権限が与えられている証明書に関してのみ表示されます。

Step 5 クラスタ内、およびでクラスタ間ピアの各 IM and Presence Service ノードに対してこの手順を繰り返し、不要な自己署名信頼証明書が展開全体で完全に削除されるようにします。

次のタスク

サービスが Tomcat である場合は、Cisco Unified Communications Manager ノード上の IM and Presence Service ノードの自己署名付き tomcat-trust 証明書を確認する必要があります。「Cisco Unified Communications Manager からの自己署名 Tomcat 信頼証明書の削除（170 ページ）」を参照してください。

Cisco Unified Communications Manager からの自己署名 Tomcat 信頼証明書の削除

クラスタ内の各ノードについて、Cisco Unified Communications Manager サービス信頼ストアには 1 つの自己署名 tomcat 信頼証明書があります。Cisco Unified Communications Manager ノードから削除する対象となるのは、これらの証明書だけです。

（注） 次の手順の情報は、-EC 証明書にも適用されます。

始める前に

CA 署名付き証明書でクラスタの IM and Presence Service ノードをすでに設定し、証明書が Cisco Unified Communications Manager ノードに伝達されるよう 30 分間待機したことを確認します。

手順

Step 1 **Cisco Unified OS 管理**で、**セキュリティ** > **証明書管理**を選択します。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

Step 2 検索結果をフィルタリングするには、ドロップダウン リストから **[証明書（Certificate）]** および **[で始まる（begins with）]** を選択し、空のフィールドに tomcat-trust と入力します。[検索（Find）] をクリックします。

[証明書の一覧（Certificate List）] ウィンドウが拡張され、tomcat-trust の証明書が示されます。

Step 3 IM and Presence Service ノードのホスト名、または名前の FQDN が含まれているリンクを特定します。これらは、このサービスおよび IM and Presence Service ノードに関連付けられている自己署名証明書です。

Step 4 IM and Presence Service ノードの自己署名 tomcat-trust 証明書のリンクをクリックします。

新しいウィンドウが表示され、tomcat-trust 証明書の詳細が示されます。

Step 5 証明書の詳細で、Issuer Name CN= と Subject Name CN= の値が一致している、つまり自己署名の証明書であることを確認します。

Step 6 自己署名の証明書であることが確認され、CA 署名付き証明書が Cisco Unified Communications Manager ノードに確実に伝達されたと判断できる場合に、**削除**をクリックします。

（注） **[削除（Delete）]**ボタンは、削除する権限が与えられている証明書に関してのみ表示されます。

Step 7 クラスタ内の各 IM and Presence Service ノードに対して、手順 4、5、および 6 を繰り返します。

証明書モニタリング タスク フロー

次のタスクを行い、証明書ステータスと有効期限を自動的にモニタするようシステムを設定します。

- 証明書の有効期限が近づいているときは、電子メールで通知する。
- 有効期限が切れた証明書を失効させる。

手順

	コマンドまたはアクション	目的
Step 1	証明書モニタ通知の設定 （171 ページ）	証明書の自動モニタリングを構成します。システムは定期的に証明書ステータスをチェックし、証明書の有効期限が近づいていると電子メールで通知します。
Step 2	OCSP による証明書失効の設定 （172 ページ）	期限切れの証明書が自動的に失効するように OCSP を設定します。

証明書モニタ通知の設定

Unified Communications Manager または IM and Presence サービスの自動証明書モニタリングを設定します。システムは定期的に証明書のステータスをチェックし、証明書の有効期限が近づいていると電子メールで通知します。

（注） [Cisco Certificate Expiry Monitor] ネットワーク サービスを実行している必要があります。デフォルトでこのサービスは有効化されていますが、**[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、[Cisco Certificate Expiry Monitor サービス（Cisco Certificate Expiry Monitor Service）] の状態が [実行中（Running）] であることを検証して Cisco Unified Serviceability でサービスが実行中であることを確認できます。

手順

Step 1 （Unified Communications Manager の証明書モニタリングのために）Cisco Unified OS の管理にログインするか、（IM and Presence サービスの証明書モニタリングのために）Cisco Unified IM and Presence の管理にログインします。

Step 2 **[セキュリティ（Security）] > [証明書モニタ（Certificate Management）]** を選択します。

Step 3 [通知開始時期（Notification Start Time）] フィールドに、数値を入力します。この値は、近づきつつある有効期限の通知を、有効期限の何日前にシステムが開始するかを表します。

Step 4 [通知頻度（Notification Frequency）] フィールドには、通知を行う頻度を入力します。

Step 5 これはオプションです。[電子メール通知を有効にする（Enable E-mail notification）] チェック ボックスをオンにして、近づきつつある証明書有効期限に関する電子メール アラートをシステムに送信させます。

Step 6 [LSC モニタリングを有効にする（Enable LSC Monitoring）] チェック ボックスをオンにして、LSC 証明書を証明書ステータス チェックに含めます。

Step 7 [電子メール ID（E-mail IDs）] フィールドに、システムが通知を送信する電子メール アドレスを入力します。複数の電子メールアドレスは、セミコロンで区切って入力できます。

Step 8 [保存（Save）] をクリックします。

（注） 証明書モニタ サービスは、デフォルトで 24 時間ごとに 1 回だけ実行します。証明書モニタ サービスを再起動すると、サービスが開始され、24時間後に実行する次のスケジュールが計算されます。証明書の有効期限が 7 日以内に近づいても、この周期は変化しません。このサービスは、証明書の有効期限が切れる 1 日前から、有効期限が切れた後も 1 時間おきに実行します。

次のタスク

Online Certificate Status Protocol（OCSP）を設定し、期限切れの証明書をシステムが自動的に失効させるようにします。詳細については、次を参照してください。 OCSP による証明書失効の設定（172 ページ）

OCSP による証明書失効の設定

オンライン証明書ステータスプロトコル（OCSP）を有効にして、証明書の状態を定期的にチェックし、期限切れの証明書を自動的に失効させます。

始める前に

システムに OCSP チェックに必要な証明書があることを確認します。OCSP 応答属性を設定されているルート CA 証明書または中間 CA 証明書を使用することができます。または、tomcat-trust へアップロードされている指定された OCSP 署名証明書を使用することができます。

手順

Step 1 （Unified Communications Manager の証明書失効のために）Cisco Unified OS の管理にログインするか、（IM and Presence サービスの証明書失効のために）Cisco Unified IM and Presence の管理にログインします。

Step 2 **[セキュリティ（Security）] > [証明書失効（Certificate Revocation）]** を選択します。

Step 3 [OCSP の有効化（Enable OCSP）] チェック ボックスをオンにして、次のタスクのいずれかを実行します。

- OCSP チェックの OCSP レスポンダを指定する場合は、[設定済み OCSP URI を使用する（Use configured OCSP URI）] ボタンを選択し、[OCSP 設定済み URI（OCSP Configured URI）] フィールドにレスポンダの URI を入力します。
- OCSP レスポンダ URI で証明書を設定する場合、[証明書からの OCSP URI を使用する（Use OCSP URI from Certificate）] ボタンを選択します。

Step 4 [失効チェックを有効にする（Enable Revocation Check）] チェック ボックスをオンにします。

Step 5 [チェック間隔（Check Every）] フィールドに失効チェックの間隔を入力します。

Step 6 [保存（Save）] をクリックします。

Step 7 （省略可）CTI、IPsec または LDAP リンクがある場合は、これらの長期性接続の OCSP 失効サポートを有効にするために、上記の手順に加えて次の手順も行う必要があります。

a) Cisco Unified CM の管理から、**[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。

b) [証明書の失効や有効期限（Certificate Revocation and Expiry）] で、[証明書有効性チェック（Certificate Validity Check）] パラメーターを [True] に設定します。

c) [有効性チェック頻度（Validity Check Frequency）] パラメーターの値を設定します。

（注） **証明書失効**ウィンドウの [失効チェックを有効にする（Enable Revocation Check）] パラメーターの間隔値は、[有効チェック頻度（Validity Check Frequency）] エンタープライズ パラメーターの値よりも優先されます。

d) [保存（Save）] をクリックします。

第 13 章

セキュリティ設定の構成

セキュリティの概要

この章では、IM and Presence Service のセキュリティ設定の設定手順について説明します。IM and Presence Service では、セキュア TLS 接続を設定し、FIPS モードなどの拡張セキュリティ設定を有効にすることができます。

IM and Presence Service が、Cisco Unified Communications Manager とプラットフォームを共有します。Cisco Unified Communications Managerのセキュリティ設定の方法の詳細は、*Cisco Unified Communications Manager* システム設定ガイド を参照してください。

セキュリティ設定のタスク フロー

このタスクを実行して、IM and Presence Service のセキュリティを設定します。

手順

	コマンドまたはアクション	目的
Step 1	ログイン バナーの作成 （176 ページ）	ユーザが IM and Presence Service インターフェイスでのログインの際に確認できるバナーを作成できます。
Step 2	セキュアな XMPP 接続の設定 （176 ページ）	このタスクを完了して、XMPP セキュリティ設定を行います。
Step 3	TLS ピア サブジェクトの設定 （178 ページ）	TLS ピアを設定する場合は、これらのタスクを設定します。
Step 4	TLS コンテキストの設定 （178 ページ）	TLS ピアの TLS コンテキストと TLS 暗号を設定します。

	コマンドまたはアクション	目的
Step 5	FIPS Mode （179 ページ）	FIPS 準拠の展開にする場合は、FIPS モードを有効にすることが可能です。セキュリティを強化するために、拡張セキュリティ モードおよび共通の準拠モードを有効にすることもできます。

ログイン バナーの作成

ユーザが IM and Presence サービス インターフェイスへのログインの一部として確認するバナーを作成できます。任意のテキスト エディタを使用して .txt ファイルを作成し、ユーザに対する重要な通知を含め、そのファイルを Cisco Unified IM and Presence OS の管理ページにアップロードします。

このバナーはすべての IM and Presence サービス インターフェイスに表示され、法的な警告や義務などの重要な情報をログインする前にユーザに通知します。Cisco Unified CM IM and Presence の管理、Cisco Unified IM and Presence オペレーティング システムの管理、Cisco Unified IM and Presence のサービスアビリティ、Cisco Unified IM and Presence のレポート、および IM and Presence のディザスタ リカバリ システム のインターフェースでは、このバナーがユーザがログインする前後に表示されます。

手順

Step 1 バナーに表示する内容を含む .txt ファイルを作成します。

Step 2 Cisco Unified IM and Presence オペレーティング システムの管理にサインインします。

Step 3 **[ソフトウェア アップグレード（Software Upgrades）] > [ログイン メッセージのカスタマイズ（Customized Logon Message）]** を選択します。

Step 4 **[参照（Browse）]** を選択し .txt ファイルを検索します。

Step 5 [ファイルのアップロード] をクリックします。

バナーは、ほとんどの IM and Presence サービス インターフェイスでログインの前後に表示されます。

（注） 「.txt」ファイルは、各 IM and Presence Service ノードに個別にアップロードする必要があります。

セキュアな XMPP 接続の設定

TLS を使用したセキュアな XMPP 接続を有効にするには、次の手順を使用します。

手順

Step 1 Cisco Unified CM IM and Presence 管理で、**システム** > **セキュリティ** > **設定**を選択します。

Step 2 適切なチェック ボックスをオンにして、以下の XMPP セキュリティ設定を有効にします。

表 *19 : IM and Presence Service* の *XMPP* セキュリティの設定

設定	説明
Enable XMPP Client To IM/P Service Secure Mode（XMPP クライアントと IM/P サービス間のセキュア モードの有効化）	有効にすると、IM and Presence Service が、クラスタの XMPP クライアント アプリケーションで、セキュアな TLS 接続を確立します。 この設定はデフォルトでイネーブルになっています。このセキュア モードをオフにしないことを推奨します。ただし、XMPP クライアント アプリケーションが非セキュア モードでクライアント ログイン クレデンシャルを保護できる場合を除きます。セキュア モードをオフにする場合は、他の方法で XMPP のクライアント ツー ノード通信を保護できることを確認してください。
Enable XMPP Router-to-Router Secure Mode（XMPP ルータツールータ セキュア モードの有効化）	この設定をオンにすると、IM and Presence サービスは同じクラスタ内または別のクラスタ内の XMPP ルータ間にセキュアな TLS 接続を確立します。IM and Presence サービスは XMPP 証明書を XMPP 信頼証明書として自動的にクラスタ内またはクラスタ間で複製します。XMPP ルータは、同じクラスタ内または別のクラスタ内にある他の XMPP ルータとの TLS 接続を確立しようとし、TLS 接続の確立に使用できます。
Enable Web Client to IM/P Service Secure Mode（Web クライアントと IM/P サービス間のセキュア モードの有効化）	この設定をオンにすると、IM and Presence サービスは、IM and Presence サービス ノードと XMPP ベースの API クライアント アプリケーション間のセキュアな TLS 接続を確立します。この設定をオンにした場合は、IM and Presence サービスの cup-xmpp-trust リポジトリに Web クライアントの証明書または署名付き証明書をアップロードします。

Step 3 **[保存（Save）]** をクリックします。

次のタスク

XMPP クライアントと IM/P サービス間のセキュア モードの有効化 設定を更新した場合、Cisco XCP Connection Manager を再起動します。

IM and Presence Service の SIP セキュリティの設定

TLS ピア サブジェクトの設定

IM and Presence サービス証明書をインポートすると、IM and Presence サービスは自動的に TLS ピア サブジェクトを TLS ピア サブジェクト リストおよび TLS コンテキスト リストに追加しようとします。要件に合わせて TLS ピア サブジェクトおよび TLS コンテキストが設定されていることを確認します。

手順

Step 1 **Cisco Unified CM IM and Presence 管理** で、**システム** > **セキュリティ** > **TLS ピア サブジェクト**を選択します。

Step 2 **[新規追加]** をクリックします。

Step 3 ピア サブジェクト名に対して次の手順のいずれかを実行します。

a) ノードが提示する証明書のサブジェクト CN を入力します。

b) 証明書を開き、CN を探してここに貼り付けます。

Step 4 [説明（Description）] フィールドにノードの名前を入力します。

Step 5 [保存（Save）] をクリックします。

次のタスク

TLS コンテキストを設定します。

TLS コンテキストの設定

TLS ピア サブジェクトに TLS コンテキストおよび TLS 暗号を割り当てるには、次の手順を使用します。

（注） IM and Presence Service証明書をインポートする際、IM and Presence Service は自動的に TLS ピア サブジェクトの TLS ピア サブジェクト リストおよび TLS コンテキスト リストへの追加を試みます。

始める前に

TLS ピア サブジェクトの設定 （178 ページ）

手順

Step 1 **Cisco Unified CM IM and Presence Administration**で、**システム** > **セキュリティ** > **TLS コンテキスト設定**を選択します。

Step 2 [検索（Find）] をクリックします。

Step 3 **[Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context]** を選択します。

Step 4 使用可能なTLSピアサブジェクトのリストから、設定したTLSピアサブジェクトを選択します。

Step 5 > の矢印を利用して、TLS ピア サブジェクトを**選択した TLS ピア サブジェクト**に移動します。

Step 6 **TLS 暗号のマッピング**の設定

a) **利用可能な TLS 暗号**および **選択した TLS 暗号** ボックスで利用できる TLS 暗号の一覧を確認します。

b) 現在選択されていない TLS 暗号を有効にするには、> 矢印を利用して、暗号を**選択した TLS 暗号**に移動します。

Step 7 **[保存（Save）]** をクリックします。

Step 8 Cisco SIP Proxy サービスを再起動します。

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ー-機能サービス（Control Center - Feature Services）]** を選択します。

b) **サーバ**ドロップダウン リスト ボックスで、IM and Presence Service クラスタ ノードを選択し、**移動**をクリックします。

c) **Cisco SIP プロキシ** サービスを選択し、**再起動**をクリックします。

FIPS Mode

IM and Presence Serviceには、一連の拡張システム セキュリティ モードが含まれています。この機能を使用すると、暗号化、データとシグナリング、および監査ログなどのアイテムを対象とした、より厳格なセキュリティ ガイドラインおよびリスク管理制御下でシステムが動作します。

- FIPS モード：IM and Presence Service を FIPS モードで動作するように設定することが可能です。これによりシステムはFIPSまたは連邦情報処理規格、米国およびカナダ政府の標準に準拠し、暗号化モジュールを使用することができます。
- 拡張セキュリティ モード：セキュリティ強化モードが FIPS 対応のシステム上で実行され、データ暗号化要件、より厳密な資格情報ポリシー、連絡先検索のためのユーザ認証、およびより厳密な監査のためのログ要件などの追加のリスク管理制御が提供されます。
- 共通基準モード：共通基準モードは、FIPS 対応システム上でも、システムを TLS や x.509 v3 証明書の使用などの一般的な基準ガイドラインに準拠するための追加制御機能を提供します。

（注） 外部データベースが MSSQL の場合、メッセージアーカイバ、テキスト会議マネージャ、ファイル転送マネージャなどのサービスを共通基準モードで動作させるには、次の手順を実行する必要があります。

1. TLS 1.1 以降をサポートするために、MSSQL データベースをホストするサーバを設定します。
2. IM and Presence サービスにデータベース証明書を再アップロードします。
3. [**External Database Configuration**] ページの [**Enable SSL**] チェックボックスをオンにします。[Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] > [メッセージ（Messaging）] > [外部サーバの設定（External Server Setup）] > [外部データベース（External Databases）] を選択して、外部データベースを設定します。

重要 この注記は、リリース 12.5(1)SU7 にのみ適用されます。

クラスタにマルチサーバーの SAN 証明書構成があり、クラスタを FIPS およびコモンクライテリアモードに移行している場合。マルチサーバー SAN 証明書が自己署名証明書に変換されます。

FIPS およびコモンクライテリアモードの Unified Communications Manager サーバーに古いマルチサーバー SAN 証明書が残っている場合は、手動で削除する必要があります。

FIPS モード、拡張セキュリティ モード、共通基準モードを Cisco Unified Communications Manager および IM and Presence Service で有効にする方法は、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html の *Cisco Unified Communications Manager* セキュリティ ガイドの「FIPS モードの設定」の章を参照してください。

FIPS の Microsoft Outlook カレンダー統合

IM and Cisco Presence サービスサーバで FIPS モードが有効になっている場合、Exchange Web サービス情報の取得にはNTLMv2だけがサポートされます。FIPSモードが無効になっている場合、既存の動作に従って NTLMv1 と NTLMv2 の両方がサポートされます。基本認証は、FIPS モードの有効化または無効化に関係なく、両方のケースでサポートされます。

Presence Engine サービスには、[FIPSモードのExchange Server認証（FIPS Mode Exchange Server Authentication）] という新しいサービス パラメータが導入されています。これにより、Microsoft Outlook カレンダー統合機能を通じて Exchange Server との接続を確立するときに Presence Engine で使用される認証の種類を確認できます。

[**FIPS Mode Exchange Server Authentication**] サービスパラメータは、[**Auto**] または [**Basic Only**] のいずれかに設定できます。

サービスパラメータが[**自動 (Auto)**]に設定されている場合:プレゼンスエンジンは、最初にntlmv2をネゴシエートし、ntlmv2 ネゴシエーションが失敗した場合にのみ「基本認証」にフォールバックします。NTLMv1 は FIPS モードではネゴシエートされません。

サービスパラメータが**基本のみ**に設定されている: プレゼンスエンジンは、Exchange サーバーが NTLM と基本認証の両方を許可するように設定されている場合でも、「基本認証」を使用するように強制されます。

（注） サービスパラメータ設定を変更する場合は、Cisco Presence エンジンを再起動する必要があります。

第 14 章

クラスタ間ピアの設定

クラスタ間ピアの概要

クラスタ間ピアリングにより、単一のクラスタ内のユーザが、同じドメイン内の別のクラスタのユーザと通信したり、プレゼンスをサブスクライブすることが可能です。大規模な導入の場合は、クラスタ間のピアリングを使用してリモート IM and Presence クラスタを接続することができます。

クラスタ間ピアリングは、ローカル クラスタおよびリモート クラスタの両方のデータベース パブリッシャーノード上で設定します。

クラスタ間展開のサイジングおよびパフォーマンスに関する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 の *Cisco Collaboration System Solution Reference Network Designs*（*SRND*） の「Collaboration Instant Messaging and Presence」の章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。

- すべてのクラスタで必要に応じてシステム 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適切に動作するには、2つのクラスタ間にファイアウォールがある場合は、次のポートを開いたままにしておく必要があります。
  - 8443（AXL）
  - 7400（XMPP）

- 5060 (SIP) SIP フェデレーションが使用されている場合のみ

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

クラスタ間ピアの設定タスク フロー

手順

	コマンドまたはアクション	目的
Step 1	ユーザプロビジョニングの確認（185 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ます。
Step 2	Cisco AXL Web サービスの有効化 （185 ページ）	Cisco AXL Web Service は、すべてのローカルおよびリモート IM and Presence ノード上で有効化されていなければなりません。サービスが実行されていることを確認するには、以下の手順を使用します。
Step 3	Sync Agent の有効化 （186 ページ）	各クラスタ間ピアのデータベース発行ノードで同期エージェントを有効にします。
Step 4	クラスタ間ピアの設定 （187 ページ）	このタスクを各クラスタのデータベースパブリッシャーノードで実行して、クラスタ ピア間の設定を行います。
Step 5	クラスタ間の Sync Agent がオンになっていることを確認 （189 ページ）	IM and Presence Service クラスタ内のすべてのノードで、クラスタ間の同期エージェントが実行されている必要があります。Intercluster Sync Agent パラメータがオンになっていることを確認します。あるいは、手動でこのサービスをオンにするには、以下の手順を使用します。
Step 6	クラスタ間ピア ステータスの確認 （190 ページ）	クラスタ間ピアの構成が動作していることを確認します。

	コマンドまたはアクション	目的
Step 7	Intercluster Sync Agent の Tomcat 信頼証明書の更新 （191 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。
Step 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 （191 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。
Step 9	クラスタ間ピアの同期間隔の設定 （192 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。
Step 10	クラスタ間ピア定期同期用の証明書の同期を無効にする （193 ページ）	この手順を使用して、クラスタ間定期同期の一部として証明書同期の無効化/有効化を設定します。

ユーザ プロビジョニングの確認

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するには、以下の手段を使用します。

手順

Step 1 Cisco Unified CM IM and Presence Administration から、 **診断** > **システムのトラブルシューティング** を選択します。
システムのトラブルシューティングが実行されます。

Step 2 **ユーザのトラブルシューティング** のセクションで、エンドユーザが適切にプロビジョニングされていること、また、重複しているユーザまたは無効なユーザがい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 （185 ページ）

Cisco AXL Web サービスの有効化

Cisco AXL Web サービスは、すべてのローカルおよびリモートIM and Presence クラスタノード上で実行されている必要があります。デフォルトでは、このサービスは実行されています。ただし、サービスが実行されていることを確認するには、以下の手順を使用することができます。

（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のアプリケーションユーザを作成します。クラスタ間ピアを設定する際には、リモートの IM and Presence Service ノードの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

Step 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。

Step 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。

Step 3 **データベースおよび管理サービス** のエリアで、**Cisco AXL Web Service**の**ステータス**を確認します。

- サービスが**開始**である場合には、作業の必要はありません。
- サービスが、**非稼働**の場合、そのサービスを選択して、**再起動**をクリックします。

Step 4 ローカル クラスタおよびリモート クラスタ内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

Sync Agent の有効化 （186 ページ）

Sync Agent の有効化

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

手順

Step 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-ネットワークサービス（Control Center - Network Services）]** を選択します。

Step 2 **サーバ** ドロップダウンリストボックスで、IM and Presence データベース パブリッシャ ノードを選択して、**移動**をクリックします。

Step 3 **IM and Presence Services**の下で、**Cisco Sync Agent** のステータスが **実行中**であることを確認します。

Step 4 サービスが、実行中でない場合には、そのサービスを選択して、**再起動**をクリックします。

Step 5 各クラスタ毎に、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 （187 ページ）

クラスタ間ピアの設定

ローカル クラスタ ノードおよびリモート クラスタの両方でこの手順を使用して、クラスタ間の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 ユーザ同期を完了する前にクラスタ間ピア接続を設定した場合、クラスタ間ピア接続のステータスは、**失敗**と表示されます。
- リモート IM and Presence Service 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があることを確認します。

手順

Step 1 Cisco Unified CM IM and Presence 管理で、**プレゼンス** > **クラスタ間設定**を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 **ピア アドレス** フィールドに、リモート クラスタのデータベース パブリッシャー ノードのノード名を入力します。このフィールドには、IP アドレス、ホスト名、または FQDN を指定することができますが、サーバを定義する実際のノード名と一致していなければなりません。

（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。

Step 4 AXL クレデンシャルを入力します。

Step 5 SIP 通信の優先 **プロトコル** を選択します。

（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には **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。

Step 6 **[保存（Save）]** をクリックします。

Step 7 GUI ヘッダーの右上にある通知を確認します。**Cisco XCP Router**を再起動するように通知された場合は、以下を実行します。それ以外の場合は、このステップは省略しても構いません。

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** ドロップダウン リスト ボックスから、IM and Presence ノードを選択して、**移動**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) 各クラスタ ノードでこの手順を繰り返します。

Step 8 各リモート クラスタ間ピアのデータベース 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、IM and Presence Service 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 接続の確立を試みます。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

クラスタ間の Sync Agent がオンになっていることを確認 （189 ページ）

XCP Router Service の再起動

ローカル クラスタ内のすべてのノードおよびリモート クラスタのすべてのノードで Cisco XCP Router サービスを再起動します。

始める前に

クラスタ間ピアの設定 （187 ページ）

手順

Step 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-ネットワークサービス（Control Center - Network Services）]** を選択します。

Step 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。

Step 3　**IM and Presence Services** エリアで、**Cisco XCP Router**を選択します。

Step 4　[再起動（Restart）] をクリックします。

次のタスク

クラスタ間の Sync Agent がオンになっていることを確認 （189 ページ）

クラスタ間の Sync Agent がオンになっていることを確認

Intercluster Sync Agent ネットワーク サービスは、クラスタ間のピア間でユーザ情報を同期します。クラスタ間の各ピア内のすべてのクラスタ ノード上でサービスが実行されていることを確認するには、以下の手順を使用します。

手順

Step 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-ネットワークサービス（Control Center - Network Services）]** を選択します。

Step 2 **サーバ** メニューから、IM and Presence Service ノードを選択して、**移動**をクリックします。

Step 3 **Cisco Intercluster Sync Agent**が **実行中**ステータスと表示されていることを確認します。

Step 4 サービスが、実行中でない場合には、そのサービスを選択して、**起動**をクリックします。

Step 5 各クラスタ間ピアのすべてのクラスタ 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 （190 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、クラスタ間ピアの設定が適切に機能していることを確認します。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**プレゼンス** > **クラスタ間設定**を選択します。

Step 2 検索条件メニューからピア アドレスを選択します。

Step 3 [検索（Find）] をクリックします。

Step 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** 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**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どうかが示されます。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通り）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。

Step 5 システムのトラブル シューティングを実行します。

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（System Troubleshooter）]** を選択します。

b) **クラスタ間トラブル シューティング** 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 （191 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に Tomcat 信頼証明書を更新するには、この手順を使用します。

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、このエラーは、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発生します。このエラーは、初めて IM and Presence をインストールする際、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

Step 1 **Cisco Unified CM IM and Presence 管理**で、**プレゼンス** > **クラスタ間設定**を選択します。

Step 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。

Step 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。

Step 4 [OK] をクリックします。

（注） 自動的に同期されない証明書がある場合は、[クラスタ間ピアの設定] ウィンドウを開きます。「X」のマークがついた証明書はすべて、証明書が欠けているため、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

Intercluster peer 周期同期が 2 時間を超える場合に、Cisco Intercluster Sync Agent で "InterClusterSyncAgentPeerPeriodicSyncingFailure" アラームが発生して自動的に再起動するようにするには、次の手順を実行します。.

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**システム** > **サービス パラメータ**を選択します。

Step 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。

Step 3 **サービス (**一覧から、**Cisco Intercluster Sync Agent**（**アクティブ**）を選択します。

Step 4 **クラスタ間のピアの周期同期障害からの自動リカバリの有効化**サービス パラメータを**有効**に設定します。

Step 5 **[保存（Save）]** をクリックします。

（注） 「クラスタ間のピアの周期同期障害からの自動リカバリの有効化」 が有効に設定されていて、定期的な同期が 2 時間以上遅延した場合：

- ***InterClusterSyncAgentPeerPeriodicSyncingFailure***アラームが生成されます。
- ***Cisco Intercluster Sync Agent*** サービスが自動的に再起動します。

[クラスタ間のピアの周期同期障害からの自動リカバリの有効化] が無効になっている場合：

- ***InterClusterSyncAgentPeerPeriodicSyncingFailure***アラームが生成されます。
- ***Cisco Intercluster Sync Agent*** サービスは自動的に再起動しません。

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

Step 1 **Cisco Unified CM IM and Presence 管理**で、**[システム（System）] > [サービスパラメータ（Service Parameters）]** を選択します。

Step 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。

Step 3 **サービス (**一覧から、**Cisco Intercluster Sync Agent**（**アクティブ**）を選択します。

Step 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。

Step 5 [保存（Save）] をクリックします。

（注） 新しい設定は、次回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。

クラスタ間ピア定期同期用の証明書の同期を無効にする

この手順を使用して、クラスタ間同期プロセスの一部として証明書の同期を無効にします。サービスパラメータ **Certificate Sync during Inter-Cluster Periodic Sync** を使用すると、管理者はクラスタ間定期同期の一部として証明書の同期を無効または有効にすることができます。このサービスパラメータのデフォルト値は、**Perform Certificate Sync** です。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**[システム（System）] > [サービスパラメータ（Service Parameters）]** を選択します。

Step 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。

Step 3 **サービス (**一覧から、**Cisco Intercluster Sync Agent**（**アクティブ**）を選択します。

Step 4 サービスパラメータ**Certificate Sync during Inter-Cluster Periodic Sync** を **Do not Perform Certificate Sync** に設定します。

Step 5 [保存（Save）] をクリックします。

（注） クラスタ間定期同期中に、証明書の同期に関連する展開でパフォーマンスの低下または高いCPUスパイクが発生した場合は、この手順を使用してサービスパラメータを設定します。

クラスタ間ピア接続を削除する

クラスタ間ピア関係を削除する場合は、次の手順を使用します。

手順

Step 1 IM and Presence Service のパブリッシャ ノードにログインします。

Step 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。

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

Step 4 [削除（Delete）] をクリックします。

Step 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 サービスは、クラスタ間ピアの削除後に IM and Presence クラスタ内の各ノードで XCP ルータが再起動しないように拡張されています。この拡張機能により、管理者は Jabber サービスを中断せずに、ノードの順次再起動によって生じるオーバーヘッドを大幅に削減することで、大規模な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の IM and Presence サービスクラスタを展開できます。これらのクラスタが集中型であるか、分散型であるかは関係ありません。
マルチクラスタ展開でのクラスタ間同期エージェントリソースの不足	ICSA を使用するには、多数のクラスタがあるマルチクラスタ導入で、より多くのリソースが必要です。リソース不足により、ICSA または SRM の問題が発生した場合。前述の Cisco SIP Proxy サービスパラメータをデフォルト値の20から新しい値10に変更することをお勧めします。 • 最大値はありません。プロセスの数 • 最大値はありません。予備のプロセス • 最大プロセス数 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。 SRM および ICSA サービスを再起動します。
クラスタ間同期エージェントと DNS	クラスタ間同期エージェントは、DNS を使用して、ピアクラスタの Tomcat 証明書（SAN エントリ）にリストされているすべての CUCM および IM&P サーバを解決します。DNS 解決が失敗した場合、クラスタ間同期エージェントはリモートピアに接続しません。

第 15 章

プッシュ通知の設定

プッシュ通知の概要

クラスタでプッシュ通知が有効になっている場合、Unified Communications Manager および IM and Presence Service は、一時停止モード（バックグラウンドモードとも呼ばれます）で動作している Android および iOS 用 Cisco Jabber または Cisco Webex クライアントに音声通話、ビデオ通話、インスタントメッセージの通知をプッシュするために、Google と Apple のクラウドベースのプッシュ通知サービスを使用します。プッシュ通知によって、システムは Cisco Jabber または Cisco Webex と永続的な通信を維持できます。プッシュ通知は、エンタープライズネットワーク内から接続する Android および iOS 用 Cisco Jabber および Cisco Webex クライアントと、Expressway のモバイルおよびリモートアクセス機能を通じてオンプレミス展開に登録するクライアントの両方で必要となります。

プッシュ通知の動作

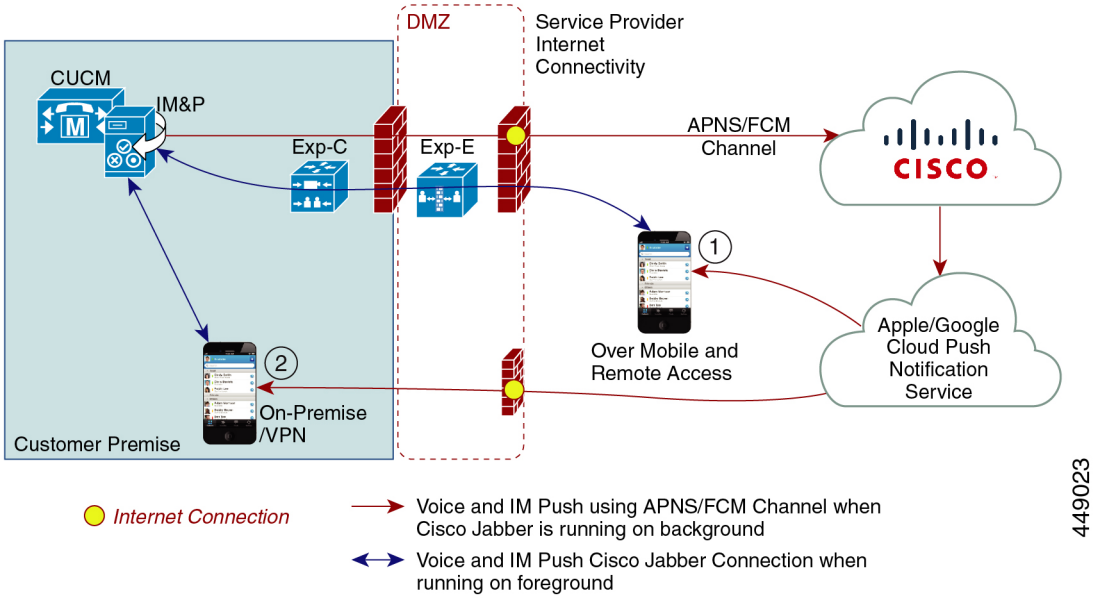
Android および iOS プラットフォームデバイスにインストールされているクライアントは、起動時に Unified Communications Manager、IM and Presence Service、および Google と Apple のクラウドに登録します。モバイルおよびリモートアクセス展開では、クライアントは Expressway 経由でオンプレミスサーバに登録します。Cisco Jabber および Cisco Webex クライアントがフォアグラウンドモードになっている限り、Unified Communications Manager および IM and Presence Service は、コールとインスタントメッセージをクライアントに直接送信することができます。

ただし、Cisco Jabber または Cisco Webex クライアントが（たとえばバッテリ寿命を長持ちさせるために）サスペンドモードに移行すると、標準の通信チャネルは使用不可となり、Unified Communications Manager および IM and Presence Service がクライアントと直接通信することはできなくなります。プッシュ通知は、パートナークラウドを介してクライアントに到達するための別のチャネルを提供します。

（注） 次の条件のいずれかに当てはまる場合、Cisco Jabber と Cisco Webex はサスペンドモードで動作していると見なされます。

- Cisco Jabber または Cisco Webex アプリケーションがオフスクリーン（バックグラウンド）で実行されている。
- Android または iOS デバイスがロックされている。
- Android または iOS デバイスの画面がオフになっている。

図 *6*: プッシュ通知アーキテクチャ



上の図は、Android および iOS 用 Cisco Jabber または Cisco Webex クライアントが、バックグラウンドで動作している場合と停止している場合の動作を示したものです。この図では、(1) クライアントが Expressway 経由でオンプレミスの Cisco Unified Communications Manager および IM and Presence Service 展開に接続するモバイルおよびリモートアクセス展開と、(2) エンタープライズネットワーク内からオンプレミス展開に直接接続する Android および iOS 用 Cisco Jabber または Cisco Webex クライアントを示しています。

（注） iOS13 の Apple クライアントおよびサポートされている Android クライアントでは、音声通話とメッセージは別々のプッシュ通知チャネル（「VoIP」と「Message」）を使用して、バックグラウンドモードで動作しているクライアントに到達します。ただし、全般的なフローはどちらのチャネルでも同じです。iOS 12 では、音声通話とメッセージは同じチャネルを使用して配信されます。

Cisco Jabber および Cisco Webex のプッシュ通知の動作

次の表は、Unified Communications Manager および IM and Presence Service に登録された iOS 用 Cisco Jabber または Cisco Webex クライアントの iOS 12 および iOS 13 での動作を説明したものです。

Cisco Jabber または Cisco Webex クライアントの動作モード	Cisco Jabber が iOS12 デバイスで実行されている場合	Cisco Jabber が iOS13 デバイスまたは Android デバイスで実行されている場合
フォアグラウンドモード	音声/ビデオ通話 Unified Communications Manager は、標準の SIP 通信チャネルを使用して、音声通話とビデオ通話を Cisco Jabber または Cisco Webex クライアントに直接送信します。 通話の場合、Unified Communications Manager はプッシュ通知もフォアグラウンドモードの Cisco Jabber または Cisco Webex クライアントに送信します。ただし、通話の確立には、プッシュ通知チャネルではなく標準の SIP チャネルが使用されます。 メッセージ IM and Presence Service は、標準の SIP 通信チャネルを使用してメッセージをクライアントに直接送信します。メッセージの場合、フォアグラウンドモードのクライアントにプッシュ通知は送信されません。	動作は iOS12 の場合と同じです。

Cisco Jabber または **Cisco Webex** クライアントの動作モード	**Cisco Jabber** が **iOS12** デバイスで実行されている場合	**Cisco Jabber** が **iOS13** デバイスまたは **Android** デバイスで実行されている場合
サスペンドモード（バックグラウンドモード）	<u>ビデオまたはビデオ コール</u> 標準の通信チャネルは使用できません。Unified CM はプッシュ通知チャネルを使用します。 通知を受信すると、Cisco Jabber または Cisco Webex クライアントは自動的にフォアグラウンドモードに戻り、クライアントが呼出音を鳴らします。 <u>メッセージ</u> 標準の通信チャネルは使用できません。IM and Presence サービスは、プッシュ通知チャネルを使用して、次のように IM 通知を送信します。 **1.** IM and Presence サービスは、Cisco Cloud のプッシュ REST サービスに IM 通知を送信します。これにより、通知が Apple クラウドに転送されます。 **2.** Apple クラウドは Cisco Jabber または Cisco Webex クライアントに IM 通知をプッシュし、Cisco Jabber または Cisco Webex クライアントに通知が表示されます。 **3.** ユーザが通知をクリックすると、Cisco Jabber または Cisco Webex クライアントは再びフォアグラウンドに移行します。Cisco Jabber または Cisco Webex クライアントは、IM and Presence Service とのセッションを再開し、インスタントメッセージをダウンロードします。 （注） Cisco Jabber または Cisco Webex クライアントがサスペンドモードの間、ユーザのプレゼンスステータスは「**退席中（Away）**」と表示されます。	iOS13 では、コールトラフィックとメッセージトラフィックは別々のプッシュ通知チャネルに分けられます。コールには「VoIP」チャネル、メッセージングには「Message」チャネルが使用されます。 <u>ビデオまたはビデオ コール</u> 標準の通信チャネルは使用できません。Unified CM は「VoIP」プッシュ通知チャネルを使用します。 VoIP 通知を受け取ると、Jabber は発信者 ID を使用して CallKit を起動します。 この動作は、Cisco Jabber または Cisco Webex iOS クライアントに適用されます。 <u>メッセージ</u> 標準の通信チャネルは使用できません。IM and Presence Service は、「Message」プッシュ通知チャネルを使用します。 **1.** IM and Presence サービスは、Cisco Cloud のプッシュ REST サービスに IM 通知を送信します。これにより、通知が Apple クラウドに転送されます。 **2.** Apple クラウドは、Cisco Jabber または Cisco Webex クライアントに IM 通知をプッシュします。 **3.** ユーザが通知をクリックすると、Cisco Jabber または Cisco Webex クライアントはフォアグラウンドモードに移行します。Cisco Jabber または Cisco Webex クライアントは、IM and Presence Service とのセッションを再開し、メッセージをダウンロードします。 （注） Cisco Jabber または Cisco Webex クライアントがサスペンドモードの間、ユーザのプレゼンスは「**退席中（Away）**」と表示されます。

プッシュ通知がサポートされるクライアント

クライアント	OS	プラットフォームクラウド	クラウドサービス
iPhone および iPad の Cisco Jabber	iOS	Apple	Appleプッシュ通知サービス（APNS）
Android の Cisco Jabber	Android	Google	Android PNS サービス
iOS での Webex	iOS	Apple	Appleプッシュ通知サービス（APNS）
Android での Webex	Android	Google	Android PNS サービス

iOS13 でのプッシュ通知の動作

iOS13 では、サスペンド状態のアプリに対するタイプ **VoIP** のプッシュ通知は、Apple によって iOS12 とは異なる方法で処理されます。2020 年 7 月以降、すべての新しいアプリおよびアプリの更新は iOS 13 SDK でビルドされています。

Cisco Unified Communications Manager および IM and Presence Service は、音声と IM メッセージの両方のプッシュに VOIP 通知チャネルを使用します。

- すべてのオーディオ/ビデオ通話に対しては、CUCM サーバがタイプ「**VoIP**」のプッシュ通知を送信します。
- すべてのメッセージに対しては、IM&P サーバがタイプ「**message**」のプッシュ通知を送信します。

CUCM は、VoIP プッシュ通知を優先順位の高い通知と見なし、遅延なしで配信します。

次の図は、**iOS12** と **iOS13** での Apple によるプッシュ通知の処理を示しています。

ここに画像を挿入

ここに画像を挿入

各ユースケースでの動作とバージョン間の相違点の詳細については、次の表を参照してください。

プッシュ通知の設定

プッシュ通知の設定および導入の方法の詳細は、『*iPhone および iPad での Cisco Jabber のプッシュ通知の導入*』（https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）を参照してください。

第 III 部

機能の設定

第 16 章

アベイラビリティおよびインスタント メッセージの設定

アベイラビリティおよびインスタントメッセージの概要

IM and Presence Service を使用すると、ユーザは自身のステータスを連絡先と共有することができます。

ポイントツーポイントインスタントメッセージ機能は、一度に2人のユーザ間のリアルタイム会話をサポートします。IM and Presence Service は、送信者から受信者へのユーザ間のメッセージを直接交換します。ポイントツーポイントのインスタントメッセージを交換するには、ユーザがインスタント メッセージクライアントでオンラインである必要があります。

インスタント メッセージング機能には、以下があります。

インスタント メッセージ フォーキング機能

複数のインスタントメッセージクライアントにログインしている連絡先にユーザがインスタントメッセージを送信すると、IM and Presence Service が各クライアントにインスタントメッセージを配信します。IM and Presence Service は、連絡先が応答するまで IM を各クライアントへのフォーキングを継続して行います。連絡先が応答すると、IM and Presence Service は連絡先が応答したクライアントのみに IM を配信します。

オフライン インスタント メッセージング

ログインしていない（オフライン）連絡先にユーザがインスタントメッセージを送信すると、IM and Presence Service はインスタント メッセージを保存し、オフラインの連絡先がインスタント メッセージ クライアントに再度サインインした際に、そのメッセージを配信します。

インスタント メッセージ のブロードキャスト

ユーザは同時に複数の連絡先に インスタント メッセージ を送信することができます。たとえば、ユーザは、大規模なグループの連絡先に通知を送信することができます。

すべてのインスタントメッセージクライアントでブロードキャストがサポートされているわけではないことに注意してください。

連絡先リストの最大サイズ

ユーザの連絡先リストの最大サイズを設定することができます。これはユーザが連絡先リストに追加することができる連絡先の数です。この設定は、Cisco Jabber クライアント アプリケーションとサードパーティ クライアント アプリケーションの連絡先リストに適用されます。

連絡先の最大数に到達したユーザは、連絡先リストに新しい連絡先を追加できず、他のユーザもそのユーザを連絡先として追加できません。ユーザが連絡先リストの最大サイズに近く、最大数を超える連絡先を連絡先リストに追加すると、IM and Presence Service は超過した連絡先を追加しません。たとえば、IM and Presence Service の連絡先リストの最大サイズが 200 であるとします。ユーザに 195 件の連絡先があり、ユーザが 6 件の新しい連絡先をリストに追加しようとすると、IM and Presence Service は 5 件の連絡先を追加し、6 件目の連絡先を追加しません。

ヒント　連絡先リストのサイズが上限に到達しているユーザがいると、**Cisco Unified CM IM and Presence 管理**のシステムのトラブルシューティングに表示されます。

アベイラビリティおよびインスタントメッセージの要件

SIP 間の IM では、以下のサービスが IM and Presence Service で実行されている必要があります。

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router

SIP と XMPP 間の IM では、以下のサービスが IM and Presence Service で実行されている必要があります。

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Router
- Cisco XCP Text Conference Manager

アベイラビリティおよびインスタントメッセージのタスク フロー

IM and Presence Service 設定のアベイラビリティおよびインスタント メッセージを設定するには、以下のタスクを実行します。

手順

	コマンドまたはアクション	目的
Step 1	プレゼンス共有の設定 （205 ページ）	プレゼンスと IM のアベイラビリティを共有するクラスタ レベルの設定を構成するには、以下の手順を使用します。プレゼンスの共有を使用すると、ユーザはお互いに IM のアベイラビリティのステータスを確認することができます。
Step 2	アドホック プレゼンス サブスクリプションの設定 （207 ページ）	一時的（アドホック）プレゼンス登録の設定この設定で、ユーザは、連絡先リストに存在しない他のユーザのプレゼンス状態を一時的に表示することができます。
Step 3	インスタント メッセージの有効化 （207 ページ）	ユーザーがインスタント メッセージを交換できるようにシステムを設定します。

プレゼンス共有の設定

プレゼンスと IM のアベイラビリティを共有するクラスタ レベルの設定を構成するには、以下の手順を使用します。プレゼンスの共有を使用すると、ユーザはお互いに IM のアベイラビリティのステータスを確認することができます。

（注） アベイラビリティの共有をオフにする場合：

- ユーザは、クライアント アプリケーションで自身のアベイラビリティのステータスを表示することができます。他のユーザのステータスは灰色で表示されます。
- ユーザがチャットルームに参加すると、アベイラビリティのステータスは、**不明**と表示されます。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**プレゼンス** > **設定** > **標準設定**を選択します。

Step 2 クラスタ全体のプレゼンス共有を有効にするには、**アベイラビリティの共有を有効にする**チェック ボックスをオンにします。

（注） 個々の Cisco Jabber ユーザは、自身の Jabber クライアントで、この設定を有効または無効にすることができます。この設定は、Cisco Jabber クライアント内でポリシー設定を再構成することによって有効または無効にすることが可能です。

Step 3 他のユーザの承認を要求せずに他のユーザのプレゼンスを表示できるようにする場合は、**確認プロンプトなしで、ユーザが他のユーザのプレゼンス ステータスを表示できるようにする**のチェックボックスをオンにします。オンにしない場合は、すべてのプレゼンス要求が他のユーザによって承認される必要があります。

（注） 個々のエンドユーザは、Cisco Jabber クライアント内でポリシー設定を再構成することによって、この設定を上書きすることができます。

Step 4 **連絡先リストの最大サイズ**および**ウォッチャの最大数（ユーザごと）**設定の最大値を構成します。最大値を使用しない場合は、**制限なし**チェック ボックスをオンにします。

Step 5 オプション。Cisco Jabber のユーザが、連絡先リストに登録されていない他のユーザのプレゼンス状態を一時的にサブスクライブできるように**アドホック プレゼンス サブスクリプションを有効にする** チェックボックスをオンにし、追加のアドホック プレゼンスを設定します。

Step 6 **プレゼンス設定** ウィンドウで、その他のすべての設定を完了します。フィールドおよびその設定についてのヘルプは、オンライン ヘルプを参照してください。

Step 7 [保存（Save）] をクリックします。

Step 8 **Cisco XCP Router** および **Cisco Presence Engine**を再起動します。

a) Cisco Unified IM and Presence Serviceability にログインして、**ツール** > **コントロール センター - 機能サービス**を選択します。
b) **Cisco Presence Engine** サービスを選択して**再起動**をクリックします。
c) **[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）]** を選択します。
d) **Cisco XCP Router** サービスを選択して、 **再起動**をクリックします。

（注） 編集したフィールドによっては、サービスを再起動する必要がない場合もあります。編集するフィールドの詳細については、オンライン ヘルプを参照してください。

次のタスク

インスタント メッセージの有効化 （207 ページ）

アドホック プレゼンス サブスクリプションの設定

アドホックプレゼンスサブスクリプションを使用すると、ユーザは、連絡先リストに登録されていない他のユーザのプレゼンス状態を一時的に表示することができます。

始める前に

プレゼンス共有の設定 （205 ページ）

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**プレゼンス** > **設定** > **標準**を選択します。

Step 2 Cisco Jabber ユーザの アドホック プレゼンス サブスクリプションをオンにするには**アドホックプレゼンスサブスクリプションを有効にする**のチェックボックスをオンにします。

Step 3 IM and Presence Service が一度に指定する実行中の一時的（アドホック）プレゼンス登録の最大数を設定します。ゼロの値を設定する場合、IM and Presence Service は実行中の一時的（アドホック）プレゼンス登録を無制限に許可します。

Step 4 一時的（アドホック）プレゼンス登録の存続可能時間値（秒単位）を設定します。

この存続可能時間値が経過すると、IM and Presence Service は一時的（アドホック）プレゼンス登録をドロップし、そのユーザのプレゼンス ステータスを一時的にモニタしなくなります。

（注） アドホック プレゼンス サブスクリプションからのインスタント メッセージがユーザーに表示されている間に存続可能時間値が経過した場合は、表示されるプレゼンス ステータスが最新でない場合があります。

Step 5 **[保存（Save）]** をクリックします。

（注） この設定では、IM and Presence Service のいずれのサービスも再起動する必要はありません。ただし、Cisco Jabber ユーザは、サインアウトしてからサインインし直して、IM and Presence Service の最新のアドホック プレゼンス サブスクリプション設定を取得する必要があります。

次のタスク

インスタント メッセージの有効化 （207 ページ）

インスタント メッセージの有効化

ユーザーがインスタント メッセージを交換できるようにシステムを設定します。

始める前に

プレゼンス共有の設定 （205 ページ）

手順

Step 1 **Cisco Unified CM IM and Presence** 管理で、**メッセージング** > **設定**を選択します。

Step 2 **インスタント メッセージングを有効にする** チェック ボックスをオンにします。

Step 3 導入のニーズに沿うチェックボックスのオプションをオンにします。フィールドの説明については、オンライン ヘルプを参照してください。

- **オフライン中の相手へのインスタントメッセージの送信を無効にする**
- **クライアントでのインスタント メッセージ履歴のログの許可（サポートされるクライアントのみ）**
- **Allow cut & paste in instant messages**

Step 4 [保存（Save）] をクリックします。

アベイラビリティおよびインスタントメッセージング連携動作および制限事項

機能	制限事項
アベイラビリティの共有	この設定をオフにすると、ユーザには自身のプレゼンス ステータスのみが表示されます。アベイラビリティ情報をクラスタ内の他のユーザと共有することはできません。また、クラスタ外から受信したアベイラビリティ情報も共有されません。
インスタント メッセージ	Cisco XCP Router が突然シャットダウンした場合、またはユーザが停止/再起動した場合、最初または停止期間中に送信されたインスタント メッセージが宛先ユーザに配信されない可能性があります。メッセージを送信したユーザに警告メッセージが送信されない場合があります。 詳細については、管理者は Cisco XCP Router のトレース ファイル rtr-jsm-1 で「Dropping packet after jsm db shutdown」を含むエラーログ行を確認できます。

第 17 章

アドホック チャットおよび常設チャットの設定

グループ チャットルームの概要

グループ チャットとは、3 人以上のユーザ間でのインスタント メッセージング セッションです。IM and Presence Service は、アドホック チャット ルームおよび常設チャット ルームをサポートします。インスタント メッセージングを有効にすると、アドホック チャット ルームのサポートがデフォルトで有効になります。ただし、常設チャット ルームのサポートについては、システムを設定する必要があります。

アドホック チャット ルーム

アドホック チャット ルームは、1 人のユーザがチャット ルームに接続されている限り存続するチャット セッションであり、最後のユーザがルームを離れると、システムから削除されます。アドホック チャットルームは、最後のユーザがルームを離れると、システムから削除されます。インスタントメッセージの会話の記録は永続的に維持されることはありません。インスタントメッセージングを有効にすると、アドホック チャット ルームはデフォルトで有効化されます。

アドホックチャットルームは、デフォルトではパブリックルームですが、プライベートに再設定することもできます。ただし、ユーザがパブリックまたはプライベートのアドホックルームに参加する方法は、使用中の XMPP クライアントのタイプによって異なります。

- 任意のアドホックチャットルーム (パブリックまたはプライベート) に参加するには、Cisco Jabber ユーザを招待する必要があります。

- サードパーティ製 XMPP クライアントのユーザは、任意のアドホックチャットルーム (パブリックまたはプライベート) に参加するために招待することができます。または、会議室ディスカバリサービスを介して参加するようにパブリック専用のアドホックルームを検索することもできます。

常設チャット ルーム

常設チャットルームは、すべてのユーザがルームを離れても存続するグループチャットセッションで、アドホック グループチャットセッションと違い、終了することはありません。ユーザは、ディスカッションを続行するために、時間が経過しても同じ会議室に戻ることが求められます。

常設チャットルームの目的は、ユーザが後で常設チャットルームに戻って、協力し合い、特定のトピックに関する知識を共有したり、そのトピックに関する発言のアーカイブを検索したり（この機能が IM and Presence Service で有効になっている場合）、そのトピックのディスカッションに参加したりできるようにすることです。

常設チャットルームにはシステムの設定が必要です。また、常設チャットでは、外部データベースを導入する必要があります。

常設チャットルームは、IOS クライアントおよび Android クライアントの両方を含め、デスクトップおよびモバイル Jabber クライアントの両方でサポートされています。モバイルクライアントの場合は、最低でも Jabber リリース 12.1 (0) を実行している必要があります。

グループ チャットの要件

アドホック チャットの要件

アドホック チャットルームを展開する場合は、インスタント メッセージングが有効になっていることを確認してください。詳細については、インスタント メッセージの有効化 （207 ページ）を参照してください。

常設チャットの要件

常設チャット ルームを展開している場合：

- インスタント メッセージングが有効になっていることを確認してください。詳細については、インスタント メッセージの有効化 （207 ページ）を参照してください。
- 外部データベースを導入する必要があります。データベースのセットアップおよびサポート情報については、http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.htmlの*IM and Presence* データベース セットアップ ガイドを参照してください。
- 常設チャットにハイ アベイラビリティを導入するかどうかを決定します。この導入タイプにより、永続的なチャットルームに冗長性およびフェール オーバーが追加されます。ただし、外部データベースの要件は、ハイ アベイラビリティを持たない機能を導入した場合と若干異なります。

• 常設チャットの展開には、少なくとも15,000 ユーザ OVA を導入することを推奨します。

グループ チャットおよび常設チャットのタスク フロー

手順

	コマンドまたはアクション	目的
Step 1	グループ チャット システム管理の設定（212 ページ）	システム管理者を追加して、常設チャット システムを管理します。
Step 2	チャット ルームの設定 （212 ページ）	常設チャット ルームの基本設定を行います。オプションとして、常設チャットを有効にします。
Step 3	Cisco XCP Text Conference Manager の再起動 （214 ページ）	常設チャットを導入する場合は、Cisco XCP Text Conference Manager サービスが実行されていることを確認します。
Step 4	常設チャット用の外部データベースの設定（214 ページ）	常設チャット ルームを使用するには、各ノードに一意の外部データベース インスタンスを設定する必要があります。 （注） 常設チャットにハイ アベイラビリティを導入している場合は、ハイ アベイラビリティの展開時のデータベース要件が若干異なるため、この章の残りのタスクはスキップすることができます。
Step 5	外部データベース接続の追加 （215 ページ）	IM and Presence Serviceで、外部データベースへの接続をセットアップします。
Step 6	常設チャット用の MSSQL データベースの Windows 認証 （215 ページ）	MSSQL 外部データベースへの接続を設定するときに、Windows 認証を有効にすることができます。
Step 7	1つの外部データベースから別のデータベースへの永続的なチャットルームの移行	IM and Presence サービスでは、すべての永続的なチャットルームとグループを既存の外部データベースから同じデータベースタイプまたは異なるタイプの別のサーバに移行します。外部データベースの移行を実行する方法の詳細については、『 Cisco IM and Presence データベースセットアップガイド 12.5 (1) SU2 リリース』の「1つの外

	コマンドまたはアクション	目的
		部データベースからの永続的なチャットルームへの移行」の項を参照してください。

グループ チャット システム管理の設定

システム管理者を追加して、常設チャット システムを管理します。

手順

Step 1 **[メッセージング（Messaging）] > [グループ チャット システムの管理者（Group Chat System Administrators）]** を選択します。

Step 2 **[Enable Group Chat System Administrators（グループ チャット システムの管理者を有効にする）]** のチェックボックスをオンにします。

設定が有効化または無効化する場合、Cisco XCP Routerを再起動する必要があります。システム管理者の設定を有効に設定すると、システム管理者を動的に追加できます。

Step 3 **[新規追加]** をクリックします。

Step 4 IM アドレスを入力します。

例

IM アドレスは name@domain の形式である必要があります。

Step 5 **ニックネーム**および**説明を入力します**。

Step 6 [保存（Save）] をクリックします。

次のタスク

チャット ルームの設定 （212 ページ）

チャット ルームの設定

ルーム メンバーおよび収容人数の設定などの基本的なチャットルームの設定と、ルームあたりのユーザの最大人数の設定を行います。

必要に応じて、**常設チャットを有効にする**チェックボックスをオンにして、常設チャットを有効にすることもできます。

手順

Step 1 Cisco Unified CM IM and Presence 管理から、**メッセージング** > **グループ チャットおよび常設チャット**を選択します。

Step 2 **プライマリグループチャットサーバのエイリアスをシステムで自動的に管理する**チェック ボックスをオンあるいはオフにして、システムがチャット ノードのエイリアスを管理するかどうかを設定します。

- オン：システムは、チャットノードエイリアスを自動的に割り当てます。これはデフォルト値です。
- オフ：管理者がチャット ノードのエイリアスを割り当てることができます。

Step 3 すべての参加者がルームから退室した後もチャットルームが存続し続けるようにするには、**常設チャットを有効にする**チェックボックスをオンにします。

（注） これはクラスタ全体の設定です。永続的なチャットがクラスタ内のいずれかのノードで有効になっている場合、任意のクラスタ内のクライアントは、ノード上のテキスト会議インスタンスとそのノードでホストされているチャットルームを検出できます。

リモートクラスタ上のユーザは、そのリモートクラスタで永続的なチャットが有効になっていなくても、ローカル クラスタ上の Text Conference インスタンスおよびチャット ルームを検出することができます。

Step 4 常設チャットを有効にするように選択した場合は、それぞれの値を以下のフィールドに設定します。

- 許可されるパーシステントチャットルームの最大数（Maximum number of persistent chat rooms allowed）
- データベース接続数
- データベース接続のハートビート間隔（秒）（Database connection heartbeat interval (seconds)）
- パーシステントチャットルームのタイムアウト値（分）（Timeout value for persistent chat rooms (minutes)）

（注） シスコのサポート担当者に連絡せずに、**データベース接続のハートビート間隔**値をゼロに設定しないでください。ハートビート間隔は、通常、ファイアウォールを介して接続を開いたままにするのに使用されます。

Step 5 **ルームの設定**で、ルームの最大数を割り当てます。

Step 6 **グループチャットおよび常設チャットの設定**ウィンドウで、残りの設定を入力します。フィールドとその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。

Step 7 [保存（Save）] をクリックします。

次のタスク

Cisco XCP Text Conference Manager の再起動 （214 ページ）

Cisco XCP Text Conference Manager の再起動

チャットの設定を編集したり、チャット ノードに複数のエイリアスを追加している場合は、**Cisco XCP Text Conference Manager** サービスを再起動します。

手順

Step 1 **Cisco Unified IM and Presence Serviceability**で、**ツール** > **コントロール センター - 機能サービス**を選択します。

Step 2 **サーバ** ドロップダウン リストから、IM and Presence ノードを選択して、**移動**をクリックします

Step 3 **IM and Presence Service** セクションで、**Cisco XCP Text Conference Manager** オプション ボタンをクリックして、**起動** あるいは **再起動**をクリックします。

Step 4 リスタートに時間がかかることを示すメッセージが表示されたら、**[OK]** をクリックします。

Step 5 （任意）サービスが完全に再起動されたことを確認するには、**[更新（Refresh）]** をクリックします。

次のタスク

常設チャットのハイアベイラビリティを導入する場合は、常設チャットのハイ アベイラビリティのタスク フロー（230 ページ）の章に進みます。

それ以外の場合は、常設チャット用の外部データベースの設定 （214 ページ）.

常設チャット用の外部データベースの設定

（注） このトピックでは、ハイ アベイラビリティを備えていない常設チャットについて説明します。常設チャットに高可用性を展開する場合は、外部データベースの設定情報ではなく、該当する章を参照してください。

常設チャットルームを設定する場合は、常設チャットルームをホストするノードごとに、個別の外部データベースインスタンスを設定する必要があります。また、次の点に注意してください。

- 永続的なチャットが有効な場合は、外部データベースを Text Conference Manager サービスに関連付ける必要があり、また、データベースがアクティブで到達可能である必要があります。そうでない場合は、Text Conference Manager は起動しません。
- 常設チャット ログ出力に外部データベースを使用する場合は、データベースが情報量を処理するのに十分な容量があることを確認します。チャット ルームのすべてのメッセージのアーカイブはオプションであり、ノードのトラフィックが増え、外部データベースのディスク領域が消費されることになります。

- 外部データベースのクリーンアップユーティリティを使用して、データベースサイズを監視するジョブを設定し、期限切れのレコードは自動的に削除します。
- 外部データベースへの接続数を設定する前に、書き込む IM の数およびそのトラフィック総量を考慮します。設定する接続数によって、システムを拡張できます。UI のデフォルト設定は、ほとんどのインストールに適していますが、特定の展開にパラメータを適応させることも可能です。

外部データベースの設定方法については、http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.htmlの*IM and Presence* サービスの外部データベースの設定ガイド を参照してください。

次のタスク

外部データベース接続の追加 （215 ページ）

外部データベース接続の追加

IM and Presence Serviceから常設チャットの外部データベースへの接続を設定します。IM and Presence サービスのクラスタ間全体には、少なくとも 1 つの一意の論理外部データベース インスタンス（テーブルスペース）が必要です。

手順

Step 1 Cisco Unified CM IM and Presence 管理で、**メッセージング** > **外部サーバの設定** > **外部データベース**を選択します。

Step 2 **[新規追加]** をクリックします。

Step 3 **データベース名** フィールドに、データベースの名前を入力します。

Step 4 **データベース タイプ** ドロップダウンから、導入する外部データベースのタイプを選択します。

Step 5 データベースの **ユーザ名** および **パスワード情報** を入力します。

Step 6 **ホスト名** フィールドにホストの DNS ホスト名または IP アドレスを入力します。

Step 7 **外部データベースの設定** ウィンドウで残りの設定を入力します。フィールドとその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。

Step 8 [保存（Save）] をクリックします。

Step 9 この手順を繰り返して、外部データベース インスタンスへの各接続を作成します。

常設チャット用の MSSQL データベースの Windows 認証

常設チャットの MSSQL 外部データベースの Windows 認証を有効にします。

Before you begin

Important リリース 14SU2 以降でサポートされます。

外部データベース接続を構成するには、「外部データベース接続の追加, on page 215」を参照してください。

Procedure

	Command or Action	Purpose
Step 1	**[データベースタイプ（Database Type）]** ドロップダウンから、外部データベースのタイプを **Microsoft SQL Server** として選択します。	
Step 2	**[Windows 認証を有効にする（Enable Windows Authentication）]** チェックボックスをオンにします。	
Step 3	**[ドメイン（Domain）]** フィールドに、Windows ドメイン名を入力します。	
Step 4	Windows ユーザの**ユーザ名**および**パスワード**情報を入力します。	**Note** Windows 認証を使用すると、ドメインレベルで Windows グループを作成でき、グループ全体の MSSQL サーバにログインを作成できます。

グループチャットと持続チャットのインタラクションと制限

表 *20 :* グループ チャットと持続チャットのインタラクションと制限

機能の相互作用	制限事項
ルームの結合のアーカイブ	ルームの入退室をアーカイブすると、トラフィックが増加し、外部データベース サーバの領域が消費されるため、これを行うかどうかは任意です。

機能の相互作用	制限事項
匿名ルームでのチャット	Cisco Jabber 経由でチャットを展開する場合（グループ チャットまたは持続チャットのいずれか）は、[グループチャットとパーシステントチャットの設定（Group Chat and Persistent Chat Settings）] ウィンドウで [デフォルトで、ルームは匿名です（Rooms are anonymous by default）] および [ルームのオーナーは、ルームを匿名にするかどうかを変更できます（Room owners can change whether or not rooms are anonymous）] オプションが選択されていないことを確認してください。いずれかのチェックボックスをオンにすると、チャットは失敗します。
データベース接続の問題	Text Conference Manager サービスが起動した後で外部データベースとの接続が失敗した場合、Text Conference Manager サービスはアクティブなままで動作を継続します。ただし、メッセージはデータベースに書き込まれなくなり、接続が回復するまで新しい永続的なルームを作成できません。
OVA 要件	常設チャットまたはクラスタ間のピアリングを導入している場合、これらの機能が導入可能な OVA サイズは 5000 ユーザ OVA になります。最低でも 15000 ユーザ OVA の導入を推奨します。集中型展開では、ユーザ ベースの規模に応じて、25000 ユーザ OVA が必要になる場合があります。OVA オプションとユーザ容量の詳細については、以下のサイトを参照してください。 （注） すべての IMP ノードに少なくとも 15000 ユーザ OVA を展開することを強く推奨します。 https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html
Microsoft SQL Server での常設チャットの文字数制限	メッセージ本文（HTML タグ + テキスト メッセージを含む）が 4000 文字を超えるチャットメッセージは配信されません。こういったメッセージは拒否され、アーカイブされません。この問題は、Microsoft SQL Server をリリース 11.5 (1) SU3 を外部データベースとして使用した場合に発生します。詳細は、CSCvd89705 を参照してください。

機能の相互作用	制限事項
ピア クラスタがサポートされていないリリースを実行している Jabber の常設チャット	Jabber モバイル用の常設チャットは、11.5 (1) SU5 で導入されています。それ以前の 11.5 (1) SU リリースではサポートされていません。この機能は、12.0 (1) または 12.0 (1) の SU1 においてもサポートされていません。 Jabber の常設チャットは今回のリリースで導入されています。Jabber Mobile用の常設チャットルームをサポートしていないピア クラスタを使用して、クラスタのトランクリングを設定している場合は、Jabber Mobile クライアントに対して以下の条件が適用されます。 常設チャット ルームが、サポートされていないリリース（11.5 (1) など）でホストされている場合： • サポートされるクラスタをホームとするJabberモバイル クライアントは、サポートされていないクラスタでホストされている常設チャットルームに参加することができます。ただし、ルームをミュートするオプションは提供されません。グローバル ミュート オプションは表示されますが、機能しません。 • サポートされていないピア クラスタをホームとするJabberモバイル クライアントは、常設チャットルームに参加することができません。 11.5 (1) SU5 など、常設チャットルームがサポートされるリリースでホストされている場合： • サポートされるクラスタをホームとするJabberモバイル クライアントの参加者は、すべての常設チャットをモバイル機能に備えています。 • サポートされないピア クラスタからのJabberモバイルクライアントは、常設チャットルームに参加することができません。 （注） 常設チャット用の検索機能は、IM 履歴が無効に設定されている Jabber 設定ファイル（*jabber-config.xml*）の場合は機能しません。
外部データベース接続および Cisco XCP Text Conferencing サービス	スプリット ブレイン現象が発生すると、サブスクライバまたはパブリッシャがピア Text Conferencing サービスを検出するか、いずれかのノードがダウンした場合、サブスクライバまたはパブリッシャは、通常の状態からバックアップへの移行を試みます。 この操作中に、ピア チャット ルームの読み込みで外部データベースへの接続に失敗した場合、Cisco XCP Text Conferencing サービスはシャットダウンします。

機能の相互作用	制限事項
ハイアベイラビリティが設定されている場合にサポートされる永続的なチャットルームの数	IM&P の導入でサポートされる永続的なチャットルームの最大数は、サブクラスタごとに5000です。 ハイアベイラビリティが有効になっている場合は、ノードごとに最大2500のルームを作成することをお勧めします。(ただし、システムはノードごとに最大5000のルームを作成できます)。ハイアベイラビリティ展開のノードごとに2500人以上のルームが設定されている場合、フェールオーバー時には、バックアップノードでホストされる会議室が5000を超えることになります。これにより、トラフィックの負荷に応じて予期しないパフォーマンスの問題が発生する可能性があります。 システム上の5000ルームの負荷は、室内の参加者の数、ルーム内のメッセージ交換の割合、およびメッセージのサイズによっても異なります。シスココラボレーションサイジングツールを使用して、永続的なチャット導入のための適切な OVA セットアップを確保します。コラボレーションサイジングツールの詳細については、次を参照してください。https://cucst.cloudapps.cisco.com/landing サブクラスタ内の両方のノード間で会議室を均等に分散させることをお勧めします。また、IM&P クラスタに複数のサブクラスタがある場合は、すべてのサブクラスタ間で会議室のロードバランスを行うことをお勧めします。現在、IM&P には、ルームのロードバランスを自動的に行うメカニズムがありません。ルームのロードバランシングの責任は、ルームを作成するユーザにあります。ルームの作成時に、ユーザは、jabber 機能を使用して、ルームの作成時にランダムなノードを自動的に選択するようにする必要があります。

機能の相互作用	制限事項
アドホックチャットルームのプライベート化	アドホックチャットルームはデフォルトでパブリックですが、メンバー用に設定できるのは次の設定のみです。 **1.** [Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] から、**[メッセージング（Messaging）]** > **[グループチャットおよび常設チャット（Group Chat and Persistent Chat）]** を選択します。 **2.** [Room are **for members only by default**] チェックボックスをオンにします。 **3.** [ルームのオーナーは、ルームをメンバー専用にするかどうかを変更できます（Room owners can change whether or not rooms are for members only）] チェックボックスをオフにします。 **4.** [他のユーザをメンバー専用ルームに招待できるのはモデレータのみです（Only moderators can invite people to members-only rooms）] チェックボックスをオフにします。 **5.** [保存（Save）] をクリックします。 **6.** Cisco XCP Text Conference サービスを再起動します。 （注） IM and Presence でアドホックチャットルームをプライベートとして設定すると、常駐なチャットルームもプライベートになります。

常設チャットの例（高可用性なし）

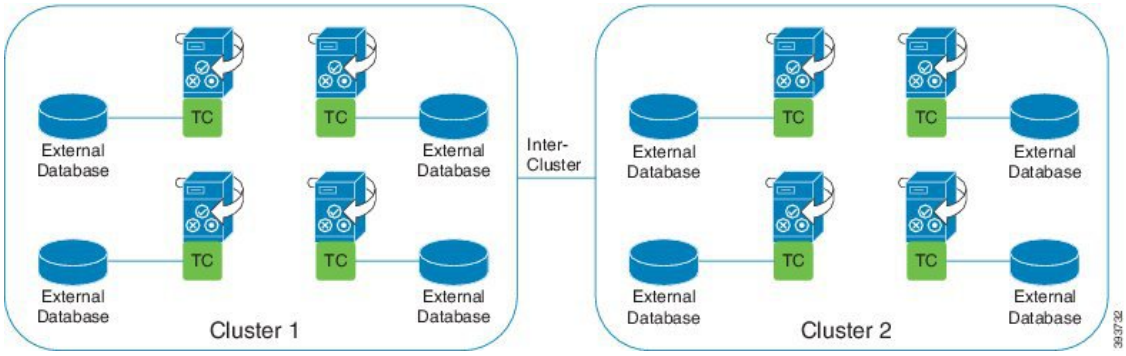
以下の 2 つの例は、常設チャットのハイ アベイラビリティが展開されていないクラスタ間のピアリングおよび常設チャットの機能を示しています。

（注） 常設チャットを導入する場合は、常設チャットのハイ アベイラビリティを提供して、常設チャット ルームに冗長性を追加することが推奨されます。

すべてのクラスタ間ノードで有効にされた常設チャット（ハイ アベイラビリティなし）

常設チャット（ハイ アベイラビリティなし）は、クラスタ ネットワーク内のすべてのノードで有効になっています。すべてのノードには、常設チャット用の外部データベースが関連付けられているため、すべてのノードで同一のチャット ルームをホストすることができます。

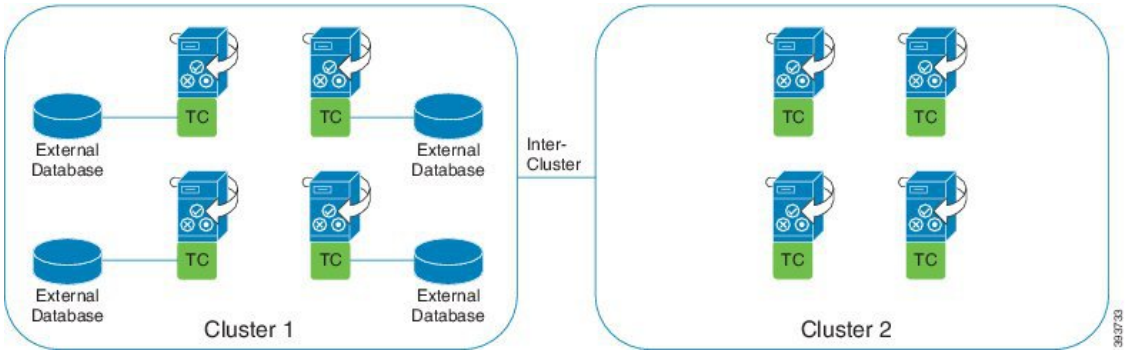
Cisco Text Conferencing サービスは、いずれかのクラスタ内のすべてのノード上で実行されています。これらのクラスタ内のすべてのユーザは、いずれかのクラスタのノードでホストされている常設チャットルームに参加することができます。



クラスタ間ネットワークの単一クラスタで有効にされた常設チャット（ハイ アベイラビリティなし）

クラスタ 1 のノードのみの外部データベースを伴う常設チャット（ハイ アベイラビリティなし）クラスタ 2 では、常設チャット ルームをホスト用にノードが設定されていないため、外部データベースは必要ありません。

ただし、Cisco Text Conference Manager サービスはいずれかのクラスタ内のすべてのノード上で実行されるため、いずれかのクラスタ内のすべてのユーザは、クラスタ 1 でホストされる常設チャットルームに参加することができます。



IM and Presence での常設チャットの境界

ここでは、さまざまな依存関係を明確化する例を使用して、IM and Presence の永続的なチャット (PChat) 境界を表すマトリックスについて説明します。

永続的なチャットの境界を導出するために、次の前提が行われます。

1. エイリアス/サーバ/サブクラスタ/クラスタあたりのルーム数に関して、次のようになります。
    1. サーバには、複数のテキスト会議エイリアスが含まれている場合があります。

2. サブクラスタには、2つのサーバ (ノード) が含まれています。
3. クラスタには、最大3つのサブクラスタを含めることができます。

2. 高可用性 (HA) が有効になっている場合、サポートされているすべての部屋番号は半減します。許可されている**常設チャットルームの最大数**の最大許容値は2500です。
3. 例: 会議室ごとに100人のユーザが平均を想定している場合、IM and Presence サービスは以下をサポートできます。
   1. 3500 HA を使用しないサーバごとの永続的なチャットルーム
   2. 1750 HA を使用したサーバごとの永続的なチャットルーム。
   3. ルームごとに1つのメッセージを1分あたり、最大273の常設チャットルームをサーバごとにアクティブにすることができます。

次に、これらの依存関係を明確化する例をいくつか示します。

タイムスライスごとにサポートされる会議室は、次の式を使用してサポートされている会議室の合計数を犠牲にすることで増やすことができます。

新しい会議室数=**現在サポートさ**れている会議室数***タイムスライスごとにサポートされる会議室の現在の数 (%) /タイムスライスごと**にサポートされる新しいルーム数 (%)

表 *21 : 25K OVA* 持続チャット容量テーブル *(サーバごと)*

ルームあたりの平均ユーザ数	サポートされている **PChat** ルームの数	タイムスライスごとにサポートされるルーム メッセージの頻度 **=1/**分	タイムスライスごとにサポートされるルーム メッセージの頻度 **=3/**分
2	5,000	100%	100 %
5	5,000	100%	58%
10	5,000	99%	33%
15	5,000	69%	23%
20	5,000	53%	18%
30	5,000	36%	12%
50	5,000	22%	7%
100	3497	16 %	5 %
200	2064	14 %	5 %
500	926	12%	4 %
1,000	482	12%	4 %

（注） ユーザの30% に2つのデバイス/クライアントがあることを前提としています。

25K OVA の例:

ルームあたりの平均ユーザー数 = 10

メッセージの頻度 = 3/分

サポートされている会議室の現在の数 = 5000

タイムスライスごとにサポートされる現在のルーム = 33%

タイムスライスごとにサポートされる新しいルーム = 50%

結果:

新しい会議室がサポートされています = 5000 * 33/50 = 3300

表 22 : 15,000 OVA* 持続チャット容量テーブル *(*サーバあたり*)

ルームあたりの平均ユーザ数	サポートされている **PChat** ルームの数	タイムスライスごとにサポートされるルーム メッセージの頻度 **=1/**分	タイムスライスごとにサポートされるルーム メッセージの頻度 **=3/**分
2	5,000	100%	80 %
5	5,000	100%	41%
10	5,000	67%	22%
15	5,000	46%	15%
20	5,000	35%	12%
30	5,000	24%	8%
50	5,000	14 %	5 %
100	3497	10 %	3 %
200	2064	9%	3 %
500	926	8%	3 %
1,000	482	7 %	2 %

（注） これは、ユーザの 30% が 2 つのデバイス/クライアントを持っていることを前提としています。

15K OVA の例:

ルームあたりの平均ユーザ数 = 5

メッセージの頻度 = 3/分

サポートされている会議室の現在の数 = 5000

タイムスライスごとにサポートされる現在のルーム = 41%

タイムスライスごとにサポートされる新しいルーム = 50%

結果:

新しい会議室がサポートされています = 5000 * 41/50 = 4100

*表 **23 : 5K OVA** 持続チャット容量テーブル (サーバごと)*

ルームあたりの平均ユーザ数	サポートされている **PChat** ルームの数	タイムスライスごとにサポートされるルーム メッセージの頻度 **=1/**分	タイムスライスごとにサポートされるルーム メッセージの頻度 **=3/**分
2	5,000	94%	31%
5	5,000	53%	18%
10	4654	33%	11%
15	4261	26%	9%
20	3929	21 %	7 %
30	3399	17%	6 %
50	2677	13 %	4 %
100	1748	10 %	3 %
200	1032	9%	3 %
500	463	8%	3 %
1,000	241	7 %	2 %

（注） これは、ユーザの 30% が 2 つのデバイス/クライアントを持っていることを前提としています。

5K OVA の例:

ルームあたりの平均ユーザ数 = 2

メッセージの頻度 = 3/分

サポートされている会議室の現在の数 = 5000

タイムスライスごとにサポートされる現在のルーム数 = 31%

タイムスライスごとにサポートされる新しいルーム = 50%

結果:

新しい会議室がサポートされています = 5000 * 31/50 = 3100

第 18 章

常設チャットのハイ アベイラビリティの設定

持続チャットにおける高可用性の概要

常設チャット用のハイアベイラビリティ（HA）は、常設チャットルームを使用しており、プレゼンス冗長グループが設定されたシステム冗長性が設定されている場合に展開することができるオプションの機能です。

常設チャットのハイ アベイラビリティは、常設チャットルームに冗長性とフェールオーバー機能を追加します。IM and Presence Service ノードの障害またはText Conferencing（TC）サービスの障害時には、サービスによりホストされるすべての常設チャット ルームが自動的にバックアップ ノードの TC サービスによってホストされます。フェールオーバー後、Cisco Jabber クライアントはシームレスに持続チャットルームを使用し続けることができます。

外部データベース

常設チャット（非HA）と常設チャットHA設定の主な違いは、外部データベースの要件にあります。

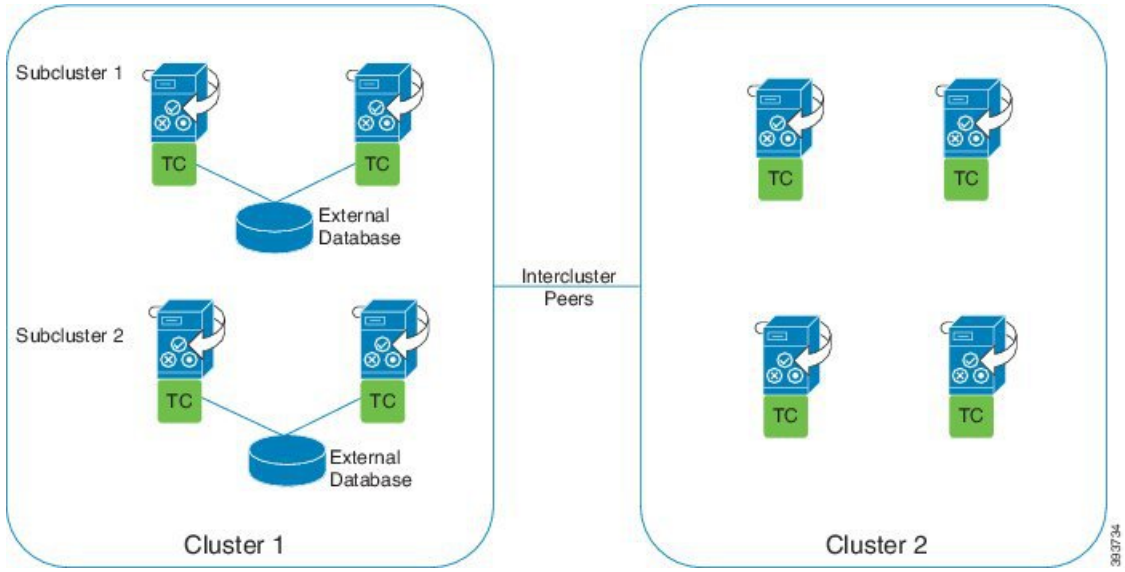
- 常設チャットが HA を使用せずに導入されている場合、外部データベースは個々のチャット ノードにのみ接続可能です。常設チャット ルームをホストする各ノードには、個別の外部データベースインスタンスが必要です。チャットノードに障害が発生すると、そのノードでホストされていた常設チャットルームは、チャットノードが復旧するまで利用できなくなります。
- 常設チャットでハイアベイラビリティが導入されている場合、外部データベースインスタンスは、サブクラスタ（プレゼンス冗長グループ）内の両方のノードに接続します。常設チャッ

トノードに障害が発生すると、サブクラスタ内のバックアップノードが引き継がれ、チャットを中断せずに続行できるようになります。

常設チャット機能のハイ アベイラビリティ：クラスタ間の例

以下の図は、常設チャットのハイ アベイラビリティがクラスタ 1 にのみ導入されているクラスタネットワークを示しています。常設チャットのハイ アベイラビリティでは、各サブクラスタが外部データベースをホストします。クラスタ 2 は、常設チャットのハイ アベイラビリティが有効にされていないため、外部データベース要件はありません。ただし、Cisco Text Conference Manager サービスがすべてのノードで実行されているため、クラスタ 2 のユーザは、クラスタ 1 にホストされている常設チャットルームに参加することができます。

（注） この例では、クラスタ 1 のチャット ルームだけが常設チャット ルームをホストする設定となっています。クラスタ 2 ノードには、常設チャットのサポートを外部データベースのインスタンスと共に追加することも可能です。この場合、いずれのクラスタのすべてのユーザが、いずれかのクラスタのいずれかのノードでホストされる常設チャットルームに参加できます。



常設チャット（非 HA）および常設チャットの HA 要件の比較

常設チャットルームを導入している場合は、常設チャットにハイアベイラビリティを導入することと、フェールオーバー機能を常設チャット ルームに追加することが推奨されます。ただし、これは必須ではありません。

次の表で、ハイ アベイラビリティを利用した、または利用せずに展開した常設チャットとの違いについて説明します。

表 *24 :* ハイ アベイラビリティを利用する場合と利用しない場合の常設チャットの比較

	常設チャット（HA なし）	常設なチャット（HA）
データベースの要件	常設チャット ルームをホストするクラスタ ノードごとに、個別の外部データベース インスタンスが必要です。この外部データベース インスタンスは、同じ外部データベース サーバ上に作成することができます。 **推奨：**最適なパフォーマンスおよびスケーラビリティを実現するために、IM and Presence のクラスタがあるノードまたは冗長性グループごとに、固有の論理外部データベース インスタンスを展開してください。ただし、これは必須ではありません。 **最小要件：** IM and Presence クラスタ ネットワークを介して常設チャットを行うには、少なくとも 1 つの外部データベース インスタンスが必要です。ただし、この導入は、使用の多いネットワークには不十分である場合があります。 **サポートされるデータベースの種類** • PostgreSql（バージョン 9.1 以降） • Oracle • Microsoft SQL Server	常設チャット ルームをホストするサブクラスタ（プレゼンス冗長性グループ）ごとに、個別の外部データベース インスタンスが必要です。この外部データベース インスタンスは、同じ外部データベース サーバ上に作成することができます。 **推奨：**最適なパフォーマンスおよびスケーラビリティを実現するために、IM and Presence クラスタ内の各サブクラスタに固有の外部データベース インスタンスを展開してください。ただし、これは必須ではありません。 **最小要件:** IM and Presence 間のクラスタネットワークには、永続的なチャット HA 用の外部データベースインスタンスが少なくとも 1 つ必要です。ただし、この導入は、使用の多いネットワークには不十分である場合があります。 **サポートされるデータベースの種類** • PostgreSql（バージョン 9.1 以降） • Oracle • Microsoft SQL Server（11.5 (1) SU2）
常設チャット ノードに障害が発生した場合の動作	• 障害が発生したノードでホストされる常設チャットルームには、ノードが復旧するまでアクセスできません。 • クラスタ冗長性が設定されていれば、障害が発生したノードに所属するユーザがサブクラスタ内のバックアップ ノードにフェールオーバーします。ただし、障害が発生したノードから常設チャット ルームにアクセスすることはできません。	• サブクラスタ内のバックアップ ノードへの常設チャット ルームのフェールオーバー。ユーザは、サービス中断なしで、メッセージングを継続することができます。 • 障害が発生したノードに所属するすべてのユーザもフェールオーバーします。

常設チャットのハイ アベイラビリティ

常設チャットのハイ アベイラビリティを設定する前に、以下を確認します。

- 常設チャット ルームが有効となっていること。詳細については、チャット ルームの設定（212 ページ）を参照してください。
- プレゼンス冗長グループに対するハイ アベイラビリティが有効となっていること。詳細については、プレゼンス冗長グループのタスク フロー（58 ページ）を参照してください。
- 外部データベースが設定されていること。データベースのセットアップおよびサポート情報については、*IM and Presence* データベース セットアップ ガイドを参照してください。

常設チャットのハイ アベイラビリティのタスク フロー

手順

	コマンドまたはアクション	目的
Step 1	外部データベースの設定 （231 ページ）	常設チャット ルームがホストされる各サブクラスタには、個別の外部データベース インスタンスが必要です。これらの個別の外部データベース インスタンスは、同じデータベースサーバ上でホストすることができます。
Step 2	外部データベース接続の追加 （231 ページ）	IM and Presence Serviceから外部データベースへの接続を設定します。
Step 3	常設チャットにおけるハイ アベイラビリティの確認 （232 ページ）	常設チャットのハイ アベイラビリティのシステム設定を確認します。
Step 4	Cisco XCP Text Conference Manager サービスの起動 （233 ページ）	Cisco XCP Text Conference Manager サービスがすべてのノードで停止した場合、この手順を使用して起動します。
Step 5	外部データベースのマージ（233 ページ）	オプション。以前のリリースからアップグレードしていて、複数の外部データベースに対して設定された常設チャットを使用している場合は、以下の手順を使用して、外部データベースを単一のデータベースにマージします。

外部データベースの設定

常設チャットにハイアベイラビリティを導入するには、常設チャットルームがホストされる各サブクラスタに対して個別の外部データベース インスタンスが必要です。これらの個別の外部データベース インスタンスは、同じデータベース サーバ上でホストすることが可能です。

サブクラスタは、IM and Presence ノード(プレゼンス Redudancy グループ)の冗長ペアです。6 ノードのIM and Presence クラスタには、最大 3 つのサブクラスタを含めることができます。6 ノードの IM and Presence クラスタで常設チャットの HA が有効になっている場合、外部データベース インスタンス 3 つと 3 つのサブクラスタ ペアが存在することになります。

外部データベース接続には、PostgreSQL、Oracle、または Microsoft SQL Server を使用することができます。セットアップの詳細については*IM and Presence* サービスのデータベース設定ガイド を参照してください。

次のタスク

外部データベース接続の追加 （231 ページ）

外部データベース接続の追加

IM and Presence Service から常設チャットの外部データベース インスタンスのハイ アベイラビリティへの接続を設定します。両方のプレゼンス冗長グループ ノードが同じ一意の論理外部データベース インスタンスに割り当てられていることを確認します。

手順

Step 1 Cisco Unified CM IM and Presence 管理で、**メッセージング** > **外部サーバの設定** > **外部データベース**を選択します。

Step 2 **[新規追加]** をクリックします。

Step 3 **データベース名** フィールドに、データベースの名前を入力します。

Step 4 **データベース タイプ** ドロップダウンから、導入する外部データベースのタイプを選択します。

Step 5 データベースの **ユーザ名** および **パスワード情報** を入力します。

Step 6 **ホスト名** フィールドにホストの DNS ホスト名または IP アドレスを入力します。

Step 7 **外部データベースの設定** ウィンドウで残りの設定を入力します。フィールドとその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。

Step 8 [保存（Save）] をクリックします。

Step 9 この手順を繰り返して、外部データベース インスタンスへの各接続を作成します。

次のタスク

常設チャットにおけるハイ アベイラビリティの確認 （232 ページ）

常設チャットにおけるハイ アベイラビリティの確認

この手順を使用して、常設チャットにハイアベイラビリティのシステム設定が行われていることを確認します。

（注） プレゼンス冗長グループ（サブクラスタ）のハイ アベイラビリティがすでに有効になっており、チャットルームの設定に常設チャットが含まれている場合は、常設チャットのハイ アベイラビリティは完了している可能性があります。

手順

Step 1 各サブクラスタでハイ アベイラビリティが有効になっていることを確認します。

a) Cisco Unified CM Administration から、**[システム（System）] > [プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。
b) **検索**をクリックして、確認するプレゼンス冗長グループを選択します。
c) **ハイ アベイラビリティの有効化**のチェックボックスを確認します。チェック ボックスがオフになっている場合は、オンにします。
d) **[保存（Save）]** をクリックします。
e) クラスタ内の各プレゼンス冗長性グループに対して、これらの手順を繰り返します。

Step 2 常設チャットが有効になっていることを確認します。

a) Cisco Unified CM 管理から、**メッセージング > グループ チャットおよび常設チャット**を選択します。
b) **常設チャットを有効にする**チェック ボックスがオンになっていることを確認します。チェック ボックスがオフになっている場合は、オンにします。
c) **[保存（Save）]** をクリックします。

Step 3 Cisco Unified CM の管理から、**Cisco XCP Text Conference Manager Service**がすべてのクラスタノード上で実行されていることを確認します。

a) **システム > プレゼンス トポロジ**を選択します。
b) クラスタ ノードごとに、**表示** をクリックしてノードの詳細情報を表示します。
c) **ノード ステータス**の下で、**Cisco XCP Text Conference Manager** サービスが**開始済**であることを確認します。
d) 左側のナビゲーション バーで、**プレゼンス トポロジ**をクリックして、クラスタ トポロジに戻り、すべてのクラスタ ノードのステータスの確認が終了するまで上記ステップを繰り返します。

次のタスク

Cisco XCP Text Conference Manager Service サービスを有効にする必要がある場合は、Cisco XCP Text Conference Manager サービスの起動 （233 ページ）。

Cisco XCP Text Conference Manager サービスの起動

Cisco XCP Text Conference Manager サービスを起動するには、この手順を使用します。このサービスは、常設チャットルームに参加できるノード上のユーザのために、すべてのクラスタノードで実行されている必要があります。

手順

Step 1 **Cisco Unified IM and Presence Serviceability**で、**ツール > コントロール センター - 機能サービス**を選択します。

Step 2 **サーバ** ドロップダウンリストで、IM and Presence クラスタ ノードを選択して、**移動** をクリックします。

Step 3 **IM and Presence Services**の下で、**Cisco XCP Text Conference Manager** を選択して、**起動** をクリックします。

Step 4 [OK] をクリックします。

Step 5 （任意）サービスが完全に再起動されたことを確認するには、**[更新（Refresh）]** をクリックします。

外部データベースのマージ

外部データベースをマージするには、以下の手順を使用します。

（注） Microsoft SQL データベースに関しては、外部データベースのマージはサポートされていません。

オプション。11.5 (1) 以前のリリースからアップグレードしており、複数の外部データベースを使用して冗長性を管理している場合は、外部データベースのマージ ツールを使用して、外部データベースを 1 つのデータベースにマージします。

例

11.5(1)以前のリリースからアップグレードしており、常設チャット ノードごとに個別の外部データベース インスタンスに接続する場合は、以下の手順を使用して、サブクラスタ内の 2 つのデータベースを 1 つのデータベースにマージして、両方のノードに接続します。

始める前に

- 2 つのソースおよび対象データベースが、プレゼンス冗長グループの各 IM and Presence Service ノードに正しく割り当てられていることを確認します。これにより両方のスキーマが有効であることが確認されます。
- 対象データベースのテーブルスペースをバックアップします。

- 対象データベース上に、新しくマージされたデータベースが十分に収まる領域があることを確認します。
- ソースデータベースと接続先データベース用に作成されたデータベースユーザに、以下のコマンドを実行する権限があることを確認します。
  - `CREATE TABLE`
  - `CREATE PUBLIC DATABASE LINK`
- データベース ユーザにこれらの権限がない場合は、次のコマンドを使用して付与することができます。
  - PostgreSQL：

    `CREATE EXTENTION`：dblink を作成し、スーパーユーザ権限または dbowner 権限を要求します。その後、次のコマンドを実行して dblink の EXECUTE 権限を付与します。

    ```
    GRANT EXECUTE ON FUNCTION DBLINK_CONNECT(text) to <user>

    GRANT EXECUTE ON FUNCTION DBLINK_CONNECT(text,text) to <user>
    ```

  - Oracle：

    ```
    GRANT CREATE TABLE TO <user_name>;

    GRANT CREATE PUBLIC DATABASE LINK TO <user_name>;
    ```

- PostgreSQL 外部データベースを使用している場合は、以下のアクセスが pg_hba ファイルに設定されていることを確認してください。
  - IM and Presence パブリッシャ ノードは、各外部データベースに対して完全なアクセス権を持っている必要があります。
  - 外部 PostgreSQL データベースには、各データベースインスタンスへの完全なアクセス権が必要です。たとえば、外部データベースが 192.168.10.1 に設定されている場合は、各データベース インスタンスが、pg_hba ファイル内で `host dbName username 192.168.10.0/24 password` と構成されていなければなりません。

手順

Step 1 IM and Presence Service パブリッシャ ノード上の [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] にサインインします。

Step 2 プレゼンス冗長グループの各 IM and Presence Service ノードの **[システム（System）] > [サービス（Services）]** ウィンドウで Cisco XCP Text Conference Service を停止します。

Step 3 **[メッセージング（Messaging）] > [外部データベースの設定（External Server Setup）] > [外部データベース ジョブ（External Database Jobs）]** をクリックします。

Step 4 マージ ジョブのリストを表示するには、[検索（Search）] をクリックします。新しいジョブを追加するには、[マージ ジョブの追加（Add Merge Job）] を選択します。

Step 5 [外部データベースのマージ（Merging External Databases）] ウィンドウで、次の情報を入力します。

- **データベース タイプ** ドロップダウンリストから**Oracle** あるいは **Postgres** を選択します。
- マージされたデータを含む2つのソース データベースと対象データベースの IP アドレスとホスト名を選択します。

[データベース タイプ（Database Type）] に [Oracle] を選択した場合、テーブルスペース名とデータベース名を入力します。[データベース タイプ（Database Type）] に [Postgres] を選択した場合、データベース名を指定します。

Step 6 [Feature テーブル（Feature Tables）] ペインで、[Text Conference（TC）] チェックボックスがデフォルトでオンになっています。現在のリリースでは、その他の選択肢はありません。

Step 7 [選択したテーブルの検証（Validate Selected Tables）] をクリックします。

（注） Cisco XCP Text Conference サービスが停止していなければ、エラー メッセージが表示されます。サービスが停止していれば、検証は完了します。

Step 8 [検証の詳細（Validation Details）] ペインにエラーがなければ、[選択したテーブルをマージ（Merge Selected Tables）] をクリックします。

Step 9 マージが正常に完了したら、[外部データベースの検索と一覧表示（Find And List External Database Jobs）] ウィンドウがロードされます。ウィンドウを更新し、新しいジョブを表示するには、[検索（Find）] をクリックします。

ウィンドウを更新し、新しいジョブを表示するには、[検索（Find）] をクリックします。

詳細を表示するには、ジョブの [ID] をクリックします。

Step 10 Cisco XCP Router サービスを再起動します。

Step 11 両方の IM and Presence Service ノードで Cisco XCP Text Conference Service を開始します。

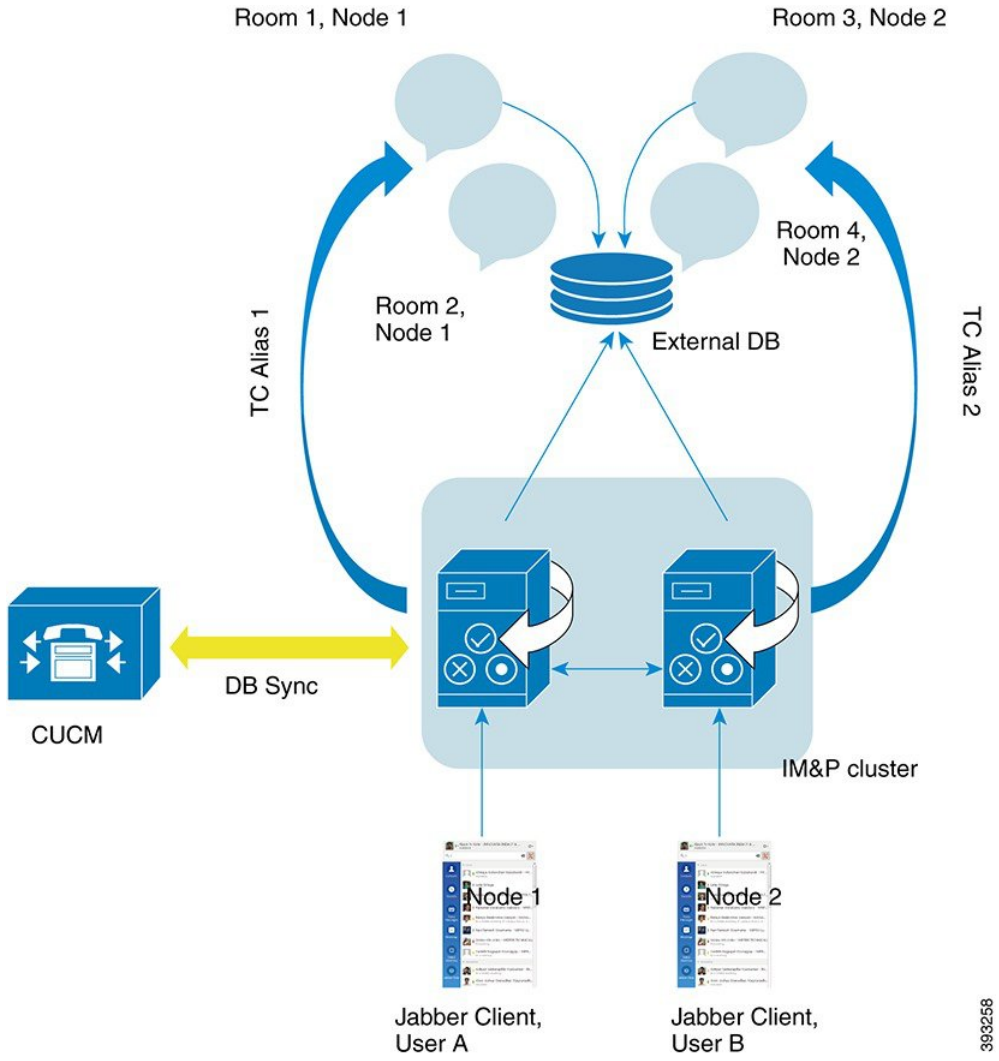
Step 12 新たにマージされた外部データベース（接続先データベース）は、プレゼンス冗長グループに再度割り当てる必要があります。

常設チャットのハイ アベイラビリティのユース ケース

次に、フェールオーバーとフェールバックにおける持続チャットの高可用性フローを示します。この例では、2 つのノードを持つ IM and Presence クラスタを対象としています。IM and Presence クラスタは、最大 6 つのノードを持つことができます。これにより、3 つのサブクラスタが可能です。常設チャットルームがすべてのノードでホストされている場合は、3 つの個別の外部データベース インスタンスが必要となります。

（注） この機能強化のために、テキスト会議（TC）サービスは不可欠なサービスとして位置付けられています。その結果、TCの高可用性のフェールオーバーのフローは、ノードの別の重要なサービス（Cisco XCP ルータ サービスなど）の障害によりフェールオーバーが引き起こされたとしても同様になります。

図 *7:* 持続チャットにおける高可用性の構造



常設チャットにおけるハイアベイラビリティのフェールオーバーユース ケース

この例では、4 人のユーザが、2 つのハイ アベイラビリティ（HA）ペアあるいはサブクラスタを持つ 4 つの IM and Presence Service ノードを持っています。ユーザは以下のように割り当てられます。

サブクラスタ 1	サブクラスタ 2
• 山田はノード1A存在：ノード1Aはチャット ルームをホストしています。 • 高橋 はノード 1B 上に	• 斎藤はノード 2A 上に存在する • 小川はノード 2B 上に存在する

1. 4 人のユーザすべてが、ノード 1A でホストされる同一のチャット ルーム内でチャットを行っています。
2. テキスト会議（TC）サービスがノード 1A で失敗します。
3. 90 秒後に、Server Recovery Manager（SRM）は TC の重要なサービスの障害を特定し、自動フェールオーバーを開始します。
4. ノード1Bは、1Aからユーザを引き継ぎ、**フェールオーバー済み**（**重要なサービスは非実行**）の状態に移行させてから、**バックアップモードで実行中** のHAの状態に移行させます。
5. HA フェールオーバー モデルに沿って、山田が自動的にログアウトし、バックアップ ノード 1B にサインインします。
6. 他のユーザは影響を受けません。ノード1B でホストされるチャットルームへのメッセージは引き続き投稿されます。
7. ユーザ A は持続チャット ルームに入り、引き続きメッセージを読んだりルームに送信したりできます。

常設チャットにおけるハイ アベイラビリティのフォールバック ユース ケース

この例では、4 人のユーザが、2 つのハイ アベイラビリティ（HA）ペアあるいはサブクラスタのある 4 つのIM and Presence Service ノードを持っています。ユーザは以下のように割り当てられます。

サブクラスタ 1	サブクラスタ 2
• 山田はノード1A存在：ノード1Aはチャット ルームをホストしています。 • 高橋 はノード 1B 上に	• 斎藤はノード 2A 上に存在する • 小川はノード 2B 上に存在する

1. 4人のユーザすべてが、ノード1Aでホストされる同一のチャットルーム内でチャットを行っています。
2. テキスト会議（TC）サービスがノード 1A で失敗します。
3. ノード 1B は、1A からユーザを引き継ぎ、**フェールオーバー済み**（**重要なサービスは非実行**）に移行させてから、**バックアップモードで実行中** のHAの状態に移行させます。
4. HAフェールオーバーモデルに沿って、山田が自動的にログアウトし、バックアップ ノード 1B にサインインします。
5. 髙橋、斎藤 および 小川は影響を受けません。ノード 1B でホストされるチャット ルームへのメッセージは引き続き投稿されます。
6. IM and Presence Service 管理者は、手動フォールバックを開始します。
7. ノード 1A は**テイクバック中**に移行して、ノード 2A は **フォールバック中**に移行します。
8. 山田はノード1Bからログアウトします。髙橋、斎藤、小川は、常設チャットルームの使用を継続し、**フォール バック** が起こると、ルームはノード 1Aに戻ります。
9. ノード 1B は、HA の状態から、 **正常**に**フォールバック**し、ピア ノード ルームをアンロードします。
10. ノード 1B は、**テイクバック中**のHA の状態から **正常**に移行し、ピア ノード ルームをリロードします。
11. ユーザ A は持続チャット ルームに入り、引き続きメッセージを読んだりルームに送信したりできます。

第 19 章

マネージド ファイル転送の設定

マネージド ファイル転送の概要

マネージド ファイル転送（MFT）を使用すると、Cisco Jabber などの IM and Presence サービス クライアントは他のユーザ、アドホック グループ チャット ルーム、および永続的なチャット ルームにファイルを転送することができます。ファイルは外部ファイル サーバのリポジトリに保存され、トランザクションが外部データベースのログに記録されます。

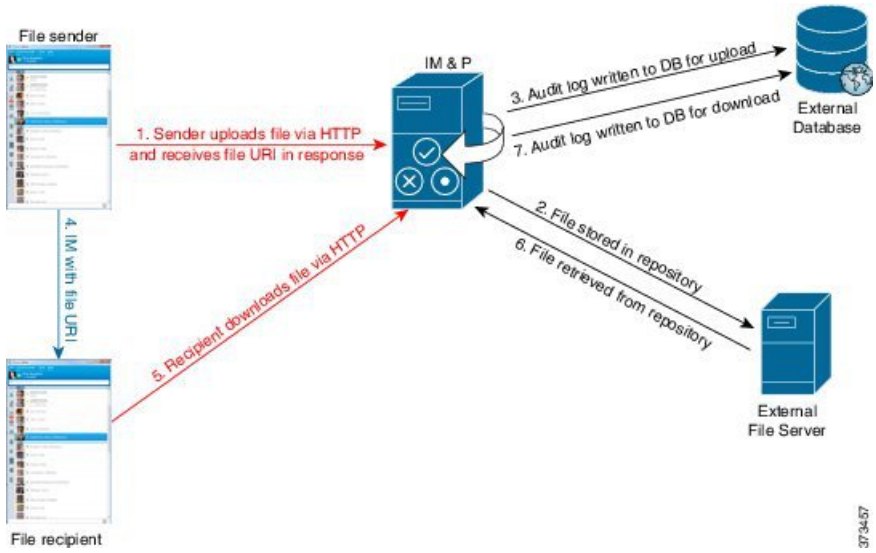
マネージド ファイル転送機能を展開するには、以下のサーバも配置する必要があります。

- **外部データベース**：すべてのファイル転送が外部データベースに記録されます。
- **外部ファイル サーバ**：転送された各ファイルのコピーを外部ファイル サーバ上のリポジトリに保存します。

（注） この設定はファイル転送に固有な設定であり、法規制コンプライアンスのためのメッセージ アーカイバ機能には影響しません。

ユース ケースついての参照先 マネージド ファイル転送の通話フロー （240 ページ）

マネージド ファイル転送の通話フロー



1. 送信者がHTTP 経由でファイルを IM and Presence Service サーバにアップロードし、サーバーはファイルの URI を応答として返します。
2. IM and Presence Service サーバーがファイルをストレージ用のファイル サーバ リポジトリに送信します。
3. IM and Presence Service が、外部データベース ログ テーブルに、アップロードを記録する項目を書き込みます。
4. 送信者は、受信者に IM を送信します。IM には、ファイルの URI が含まれています。
5. 受信者は、このファイルの IM and Presence Service に HTTP 要求を送信します。IM and Presence Service が、リポジトリからファイルを読み取り（6）、ログ テーブルにダウンロードを記録（7）した後で、ファイルが受信者にダウンロードされます。

グループチャットや常設チャットルームにファイルを転送するためのフローもこれと類似していますが、異なる点として送信者はチャット ルームに IM を送信し、チャット ルームの各参加者は個別にファイル ダウンロード要求を送信します。

（注） ファイルのアップロードが発生すると、そのドメインで使用可能な企業内のすべてのマネージドファイル転送サービスの中からマネージドファイル転送サービスが選択されます。ファイル アップロードは、このマネージドファイル転送サービスを実行しているノードに関連付けられた外部データベースと外部ファイル サーバのログに記録されます。あるユーザがこのファイルをダウンロードすると、この2番目のユーザのホームがどこかにあるかには関係なく、同じマネージドファイル転送サービスがその要求を処理して、同じ外部データベースおよび同じ外部ファイル サーバのログに記録します。

マネージド ファイル転送の要件

- 外部データベースおよび外部ファイル サーバも配置する必要があります。
- すべてのクライアントが、割り当てられている IM and Presence Service ノードの完全な FQDN を解決できることを確認してください。これは、マネージド ファイル転送の動作のために必要とされます。

外部データベースの要件

ヒント　また、常設チャットやメッセージ アーカイバを導入している場合は、すべての機能に同じ外部データベースとファイル サーバを割り当てることができます。サーバ容量を判断する際には、見込まれる IM トラフィック、ファイル転送数、およびファイル サイズを考慮する必要があります。

外部データベースをインストールして設定します。サポートされるデータベースを含む詳細は、*IM and Presence* データベース セットアップ ガイド を参照してください。

さらに、以下のガイドラインに従ってください。

- IM and Presence サービス クラスタ内の各 IM and Presence サービス ノードに対して 1 つの固有の論理外部データベース インスタンスが必要です。
- 外部データベースは、仮想化プラットフォームと非仮想化プラットフォームの両方でサポートされています。
- ログに記録されるメタデータの完全なリストについては、*Cisco Unified Communications Manager* での *IM and Presence Service* のデータベース設定ガイドの「外部データベースツール」の AFT_LOG テーブルを参照してください。
- IPv6 を使用して外部データベースに接続する場合は、IPv6 のセットアップの詳細について IPv6 の設定タスクフロー（40 ページ） を確認してください。

外部ファイル サーバの要件

外部ファイル サーバをセットアップする際は、以下のガイドラインに従ってください。

- ファイルサーバーの容量に応じて、各 IM and Presence Service ノードは独自の Cisco XCP File Transfer Manager ファイル サーバ ディレクトリを必要とします。ただし、複数のノードで同じ物理ファイル サーバ インストールを共有することもできます。
- ファイルサーバーは ext4 ファイル システム、SSHv2、および SSH ツールをサポートする必要があります。
- ファイルサーバーは、4.9、6.x、and 7.x の OpenSSH バージョンをサポートする必要があります。

重要 このノートは、リリース 14SU3 以降に適用されます。

（注） OpenSSH バージョン 8.x は、リリース 14SU3 以降でサポートされています。

- IM and Presence Service と外部ファイル サーバの間のネットワーク スループットは、1 秒間に 60 MB を超えている必要があります。

  ファイル サーバの転送スピードを判別するために、マネージドファイル転送を有効化した後で、show fileserver transferspeed CLI コマンドを使用できます。なお、システムの稼動率が高いときにこのコマンドを実行すると、コマンドから返される値に影響を与えることがあります。このコマンドの詳細については、このリンクの *Cisco Unified Communications Solutions* コマンドライン インタフェイス ガイド を参照してください。

外部ファイル サーバのパーティション

サーバ上で稼動している他のアプリケーションが書き込まないように、ファイル転送ストレージ専用の別のパーティションを 1 つ以上作成することをシスコでは推奨しています。すべてのファイル ストレージ ディレクトリを、これらのパーティションに作成してください。

次の例をご覧ください。

- パーティションを作成する場合、IM and Presence Service のデフォルト ファイル サイズ（0）を設定すると、最大 4 GB までファイルを転送できることに注意してください。マネージドファイル転送をセットアップするときには、この設定を低い値にすることができます。
- 1 日あたりのアップロード数と平均ファイル サイズを考慮してください。
- 予想されるファイル容量を保持するのに十分なディスク領域がパーティションにあることを確認します。
- たとえば 12000 人のユーザが 1 時間あたり平均 100 KB のファイルを 2 つ転送すると、1 日 8 時間では 19.2 GB になります。

外部ファイル サーバのディレクトリ構造

次の例に示すように、最初のファイル転送が発生すると、タイムスタンプ付きのサブディレクトリが自動生成されます。

- IM and Presence Service ノード上にパス `/opt/mftFileStore/node_1/` を作成します。
- ディレクトリ `/files/` が自動生成されます。
- 3 つの `/chat_type/` ディレクトリ（`im`、`persistent`、`groupchat`）が自動的に生成されます。
- 日付のディレクトリ `/YYYYMMDD/` が自動生成されます。

- 時間のディレクトリ /HH/ が自動生成されます。1 時間以内に 1,000 個を超えるファイルが転送されると、追加のロールオーバー ディレクトリ /HH.n/ が作成されます。
- ファイルは、自動生成されたエンコード リソース名付きで保存されます（これ以降、file_name と表します）。

この例では、ファイルの完全パスは /opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name となります。

この例のパスを使用すると：

- 2014 年 8 月 11 日 15.00 ～ 15.59 UTC に 1 対 1 の IM で転送されたファイルは、以下のディレクトリに配置されます。/opt/mftFileStore/node_1/files/im/20140811/15/file_name

  2014 年 8 月 11 日 16.00 ～ 16.59 UTC に常設グループ チャットで転送されたファイルは、以下のディレクトリに配置されます。/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name
- 2014 年 8 月 11 日 16.00 ～ 16.59 UTC にアドホック チャットで転送された 1001 番目のファイルは、以下のディレクトリに配置されます。/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name
- 1 時間単位の中でファイル転送が発生しない場合、その期間にはディレクトリが作成されません。

（注） IM and Presence Service とファイル サーバの間のトラフィックは SSHFS を使用して暗号化されますが、ファイルの内容は、暗号化されていない形式でファイル サーバに書き込まれます。

外部ファイル サーバのユーザ認証

IM and Presence Service は、次のように SSH キーを使用して自身とファイル サーバを認証します。

- IM and Presence Service のパブリック キーはファイル サーバに保存されます。
- SSHFS は、接続中に IM and Presence Service のプライベート キーを検証します。これで、すべてのファイルの内容が確実に暗号化されます。
- ファイル サーバのパブリック キーは、IM and Presence Service に格納されます。これにより IM and Presence Service は設定済みのファイル サーバに確実に接続し、中間者攻撃を最小限に抑えることができます。

（注） ノードの公開キーはノードの割り当てが解除されると無効になります。ノードが再び割り当てられると、新しいノード公開キーが自動的に生成されます。このキーを外部ファイル サーバで再設定する必要があります。

外部ファイル サーバの要件

外部ファイル サーバをセットアップする際は、以下のガイドラインに従ってください。

- ファイルサーバーの容量に応じて、各 IM and Presence Service ノードは独自の Cisco XCP File Transfer Manager ファイル サーバ ディレクトリを必要とします。ただし、複数のノードで同じ物理ファイル サーバ インストールを共有することもできます。
- ファイルサーバーは ext4 ファイル システム、SSHv2、および SSH ツールをサポートする必要があります。
- ファイルサーバーは、4.9、6.x、and 7.x の OpenSSH バージョンをサポートする必要があります。

重要 このノートは、リリース 14SU3 以降に適用されます。

（注） OpenSSH バージョン 8.x は、リリース 14SU3 以降でサポートされています。

- IM and Presence Service と外部ファイル サーバの間のネットワーク スループットは、1 秒間に 60 MB を超えている必要があります。

  ファイル サーバの転送スピードを判別するために、マネージドファイル転送を有効化した後で、show fileserver transferspeed CLI コマンドを使用できます。なお、システムの稼動率が高いときにこのコマンドを実行すると、コマンドから返される値に影響を与えることがあります。このコマンドの詳細については、このリンクの *Cisco Unified Communications Solutions* コマンドライン インタフェイス ガイド を参照してください。

外部ファイル サーバのパーティション

サーバ上で稼動している他のアプリケーションが書き込まないように、ファイル転送ストレージ専用の別のパーティションを 1 つ以上作成することをシスコでは推奨しています。すべてのファイル ストレージ ディレクトリを、これらのパーティションに作成してください。

次の例をご覧ください。

- パーティションを作成する場合、IM and Presence Service のデフォルト ファイル サイズ（0）を設定すると、最大 4 GB までファイルを転送できることに注意してください。マネージドファイル転送をセットアップするときには、この設定を低い値にすることができます。
- 1 日あたりのアップロード数と平均ファイル サイズを考慮してください。
- 予想されるファイル容量を保持するのに十分なディスク領域がパーティションにあることを確認します。

- たとえば 12000 人のユーザが 1 時間あたり平均 100 KB のファイルを 2 つ転送すると、1 日 8 時間では 19.2 GB になります。

外部ファイル サーバのディレクトリ構造

次の例に示すように、最初のファイル転送が発生すると、タイムスタンプ付きのサブディレクトリが自動生成されます。

- IM and Presence Service ノード上にパス `/opt/mftFileStore/node_1/` を作成します。
- ディレクトリ `/files/` が自動生成されます。
- 3 つの `/chat_type/` ディレクトリ（`im`、`persistent`、`groupchat`）が自動的に生成されます。
- 日付のディレクトリ `/YYYYMMDD/` が自動生成されます。
- 時間のディレクトリ `/HH/` が自動生成されます。1 時間以内に 1,000 個を超えるファイルが転送されると、追加のロールオーバー ディレクトリ `/HH.n/` が作成されます。
- ファイルは、自動生成されたエンコード リソース名付きで保存されます（これ以降、`file_name` と表します）。

この例では、ファイルの完全パスは `/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name` となります。

この例のパスを使用すると：

- 2014 年 8 月 11 日 15.00 ～ 15.59 UTC に 1 対 1 の IM で転送されたファイルは、以下のディレクトリに配置されます。`/opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  2014 年 8 月 11 日 16.00 ～ 16.59 UTC に常設グループ チャットで転送されたファイルは、以下のディレクトリに配置されます。`/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`
- 2014 年 8 月 11 日 16.00 ～ 16.59 UTC にアドホック チャットで転送された 1001 番目のファイルは、以下のディレクトリに配置されます。`/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- 1 時間単位の中でファイル転送が発生しない場合、その期間にはディレクトリが作成されません。

（注） IM and Presence Service とファイル サーバの間のトラフィックは SSHFS を使用して暗号化されますが、ファイルの内容は、暗号化されていない形式でファイル サーバに書き込まれます。

外部ファイル サーバのユーザ認証

IM and Presence Service は、次のように SSH キーを使用して自身とファイル サーバを認証します。

- IM and Presence Service のパブリック キーはファイル サーバに保存されます。
- SSHFS は、接続中に IM and Presence Service のプライベート キーを検証します。これで、すべてのファイルの内容が確実に暗号化されます。
- ファイル サーバのパブリック キーは、IM and Presence Service に格納されます。これにより IM and Presence Service は設定済みのファイル サーバに確実に接続し、中間者攻撃を最小限に抑えることができます。

（注） ノードの公開キーはノードの割り当てが解除されると無効になります。ノードが再び割り当てられると、新しいノード公開キーが自動的に生成されます。このキーを外部ファイル サーバで再設定する必要があります。

外部ファイル サーバのパーティション推奨

サーバ上で稼動している他のアプリケーションが書き込まないように、ファイル転送ストレージ専用の別のパーティションを 1 つ以上作成することをシスコでは推奨しています。すべてのファイル ストレージ ディレクトリを、これらのパーティションに作成してください。

次の例をご覧ください。

- パーティションを作成する場合、IM and Presence Service のデフォルト ファイル サイズ（0）を設定すると、最大 4 GB までファイルを転送できることに注意してください。マネージド ファイル転送をセットアップするときには、この設定を低い値にすることができます。
- 1 日あたりのアップロード数と平均ファイル サイズを考慮してください。
- 予想されるファイル容量を保持するのに十分なディスク領域がパーティションにあることを確認します。
- たとえば 12000 人のユーザが 1 時間あたり平均 100 KB のファイルを 2 つ転送すると、1 日 8 時間では 19.2 GB になります。

外部ファイル サーバのユーザ認証

IM and Presence Service は、次のように SSH キーを使用して自身とファイル サーバを認証します。

- IM and Presence Service のパブリック キーはファイル サーバに保存されます。
- SSHFS は、接続中に IM and Presence Service のプライベート キーを検証します。これで、すべてのファイルの内容が確実に暗号化されます。
- ファイル サーバのパブリック キーは、IM and Presence Service に格納されます。これにより IM and Presence Service は設定済みのファイル サーバに確実に接続し、中間者攻撃を最小限に抑えることができます。

（注） ノードの公開キーはノードの割り当てが解除されると無効になります。ノードが再び割り当てられると、新しいノード公開キーが自動的に生成されます。このキーを外部ファイル サーバで再設定する必要があります。

外部ファイル サーバ ディレクトリ構造

次の例に示すように、最初のファイル転送が発生すると、タイムスタンプ付きのサブディレクトリが自動生成されます。

- IM and Presence Service ノード上にパス /opt/mftFileStore/node_1/ を作成します。
- ディレクトリ /files/ が自動生成されます。
- 3 つの /chat_type/ ディレクトリ（im、persistent、groupchat）が自動的に生成されます。
- 日付のディレクトリ /YYYYMMDD/ が自動生成されます。
- 時間のディレクトリ /HH/ が自動生成されます。1 時間以内に 1,000 個を超えるファイルが転送されると、追加のロールオーバー ディレクトリ /HH.n/ が作成されます。
- ファイルは、自動生成されたエンコード リソース名付きで保存されます（これ以降、file_name と表します）。

この例では、ファイルの完全パスは /opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name となります。

この例のパスを使用すると：

- 2014 年 8 月 11 日 15.00 ～ 15.59 UTC に 1 対 1 の IM で転送されたファイルは、以下のディレクトリに配置されます。/opt/mftFileStore/node_1/files/im/20140811/15/file_name

  2014 年 8 月 11 日 16.00 ～ 16.59 UTC に常設グループ チャットで転送されたファイルは、以下のディレクトリに配置されます。/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name
- 2014 年 8 月 11 日 16.00 ～ 16.59 UTC にアドホック チャットで転送された 1001 番目のファイルは、以下のディレクトリに配置されます。/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name
- 1 時間単位の中でファイル転送が発生しない場合、その期間にはディレクトリが作成されません。

（注） IM and Presence Service とファイル サーバの間のトラフィックは SSHFS を使用して暗号化されますが、ファイルの内容は、暗号化されていない形式でファイル サーバに書き込まれます。

マネージド ファイル転送のタスク フロー

これらのタスクを完了して、IM and Presence Serviceのマネージド ファイル転送機能を設定し、外部ファイル サーバを設定します。

始める前に

マネージドファイル転送用の外部データベースと外部ファイルサーバを設定します。要件については、以下を参照してください。

- 外部データベースの要件 （241 ページ）
- 外部ファイル サーバの要件 （241 ページ）

外部データベースの設定方法の詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.htmlの *IM and Presence Service* 外部データベース セットアップ ガイドを参照してください。

手順

	コマンドまたはアクション	目的
Step 1	外部データベース接続の追加 （249 ページ）	IM and Presence Serviceから外部データベースへの接続を設定します。
Step 2	外部ファイル サーバのセットアップ（249 ページ）	ファイル サーバ上でユーザ、ディレクトリ、帰属、権限、および他のタスクを設定する前に、以下の手順を実行します。
Step 3	外部ファイル サーバのユーザの作成（251 ページ）	外部ファイル サーバのユーザを作成します。
Step 4	外部ファイルサーバのディレクトリのセットアップ （252 ページ）	外部ファイルサーバの最上位レベルのディレクトリ構造を設定します。
Step 5	外部ファイル サーバの公開キーの取得 （253 ページ）	外部ファイル サーバ 公開キーを取得します。
Step 6	IM and Presence Service での外部ファイル サーバのプロビジョニング （254ページ）	外部ファイル サーバに関する以下の情報を取得します。
Step 7	Cisco XCP File Transfer Manager のアクティベーションの確認 （256 ページ）	マネージド ファイル転送が有効になっている各ノードで、Cisco XCP File Transfer Managerサービスが有効化されていなければなりません。

	コマンドまたはアクション	目的
Step 8	マネージド ファイル転送の有効化（257 ページ）	IM and Presence Serviceでのマネージドファイル転送を有効にします。
Step 9	外部サーバのステータスの確認（259 ページ）	外部データベースの設定と外部ファイル サーバの設定に問題がないことを確認します。

外部データベース接続の追加

IM and Presence Serviceから外部データベースへの接続を設定します。マネージドファイル転送では、各 IM and Presence Service ノードに対して 1 つの固有の論理外部データベース インスタンスが必要です。

始める前に

各外部データベースの設定詳細については、以下の *IM and Presence Service* 外部データベース セットアップ ガイドを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

手順

Step 1 Cisco Unified CM IM and Presence 管理で、**メッセージング** > **外部サーバの設定** > **外部データベース**を選択します。

Step 2 **[新規追加]** をクリックします。

Step 3 **データベース名** フィールドに、データベースの名前を入力します。

Step 4 **データベース タイプ** ドロップダウンから、導入する外部データベースのタイプを選択します。

Step 5 データベースの **ユーザ名** および **パスワード情報** を入力します。

Step 6 **ホスト名** フィールドにホストの DNS ホスト名または IP アドレスを入力します。

Step 7 **外部データベースの設定** ウィンドウで残りの設定を入力します。フィールドとその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。

Step 8 [保存（Save）] をクリックします。

Step 9 この手順を繰り返して、外部データベース インスタンスへの各接続を作成します。

外部ファイル サーバのセットアップ

ファイル サーバ上でユーザ、ディレクトリ、帰属、権限、および他のタスクを設定する前に、以下の手順を実行します。

始める前に

外部ファイルサーバの設計上の推奨事項を確認します。詳細については、外部ファイルサーバの要件（241 ページ）を参照してください。

手順

Step 1 サポート対象のバージョンの Linux をインストールします。

Step 2 次のいずれかのコマンドを root として入力し、ファイルサーバーが SSHv2 および OpenSSH 4.9 以降をサポートしていることを確認します。

```
# telnet localhost 22
Trying ::1...
Connected to localhost.
Escape character is '^]'.
SSH-2.0-OpenSSH_5.3
```

または

```
# ssh -v localhost
OpenSSH_5.3p1, OpenSSL 1.0.0-fips 29 Mar 2010
debug1: Reading configuration data /root/.ssh/config ...
...debug1: Local version string SSH-2.0-OpenSSH_5.3
...
```

Step 3 プライベート/パブリック キーの認証を許可するには、`/etc/ssh/sshd_config` ファイルで以下のフィールドが *yes* に設定されていることを確認します。

- RSAAuthentication *yes*
- PubkeyAuthentication *yes*

ファイル内でこれらの行をコメント アウトした場合、設定をそのまま保持することが可能です。

ヒント また、セキュリティを強化するために、ファイル転送ユーザ（この例では *mftuser*）に対してパスワードログインを無効にすることもできます。これにより、必ずSSHのパブリック/プライベート キー認証によってログインされるようになります。

Step 4 サーバ上で稼動している他のアプリケーションが書き込まないように、ファイル転送ストレージ専用の別のパーティションを 1 つ以上作成することをシスコでは推奨しています。すべてのファイル ストレージ ディレクトリを、これらのパーティションに作成してください。

次のタスク

外部ファイル サーバのユーザの作成（251 ページ）

外部ファイル サーバのユーザの作成

外部ファイル サーバのユーザを作成します。

始める前に

外部ファイル サーバのセットアップ（249 ページ）

手順

Step 1 ファイル サーバ上で root として、マネージド ファイル転送機能用のユーザを作成します。このユーザは、ファイル ストレージのディレクトリ構造を所有し（この例では *mftuser* を使用）、強制的にホーム ディレクトリを作成します（**-m**）。

```
# useradd -m mftuser
# passwd mftuser
```

Step 2 マネージド ファイル転送ユーザに切り替えます。

```
# su mftuser
```

Step 3 *~mftuser* ホーム ディレクトリの下に、キー ストアとして使用する .ssh ディレクトリを作成します。

```
$ mkdir ~mftuser/.ssh/
```

Step 4 .ssh ディレクトリの下に authorized_keys ファイルを作成します。このファイルは、マネージド ファイル転送が有効になっている各ノードについて、パブリック キーを保持するのに使われます。

```
$ touch ~mftuser/.ssh/authorized_keys
```

Step 5 パスワードを使用しない SSH が機能するように、正しい権限を設定します。

```
$ chmod 700 ~mftuser (directory)
$ chmod 700 ~/.ssh (directory)
$ chmod 700 ~/.ssh/authorized_keys (file)
```

（注） いくつかの Linux システムでは、SSH の設定によってこれらの権限が異なることがあります。

次のタスク

外部ファイル サーバのディレクトリのセットアップ（252 ページ）

外部ファイル サーバのディレクトリのセットアップ

外部ファイル サーバの最上位レベルのディレクトリ構造を設定します。

任意のディレクトリ名を付けて、任意のディレクトリ構造を作成することができます。必ずマネージドファイル転送が有効になっている各ノード用にディレクトリを作成してください。後に、IM and Presence Service でマネージド ファイル転送を有効にする際には、各ディレクトリをノードに割り当てる必要があります。

重要 マネージド ファイル転送が有効になっている各ノード用に 1 つのディレクトリを作成する必要があります。

（注） ファイル サーバのパーティション/ディレクトリは、ファイルの格納に使用される IM and Presence Service ディレクトリにマウントされます。

始める前に

外部ファイル サーバのユーザの作成（251 ページ）

手順

Step 1 root ユーザーに切り替えます。

```
$ exit
```

Step 2 マネージド ファイル転送が有効になっている IM and Presence Service のすべてのノードのディレクトリを格納するために、最上位のディレクトリ構造（この例では `/opt/mftFileStore/`）を作成します。

```
# mkdir -p /opt/mftFileStore/
```

Step 3 `/opt/mftFileStore/` の占有者として *mftuser* を指定します。

```
# chown mftuser:mftuser /opt/mftFileStore/
```

Step 4 *mftuser* に、`mftFileStore` ディレクトリに対する占有権を付与します。

```
# chmod 700 /opt/mftFileStore/
```

Step 5 *mftuser* に切り替えます。

```
# su mftuser
```

Step 6 マネージド ファイル転送が有効になっている各ノードに関して、`/opt/mftFileStore/` の下にサブディレクトリを作成します（後で、マネージド ファイル転送を有効にするときに各ディレクトリを 1 つのノードに割り当てます）。

```
$ mkdir /opt/mftFileStore/{node_1,node_2,node_3}
```

（注）
- これらのディレクトリおよびパスは、Cisco Unified CM IM and Presence 管理ページでファイルサーバをプロビジョニングする際に設定する **外部ファイル サーバ ディレクトリ** フィールドで使用されます。
- 複数の IM and Presence Service ノードがこのファイル サーバに書き込む場合は、前述の例で 3 つのノード {*node_1*,*node_2*,*node_3*} に設定したように、各ノードのターゲット ディレクトリを定義する必要があります。
- 各ノードのディレクトリ内では、転送タイプのサブディレクトリ（`im`、`groupchat`、および `persistent`）が IM and Presence Service によって自動的に作成されます。その後のすべてのディレクトリも同様です。

次のタスク

外部ファイル サーバの公開キーの取得（253 ページ）

外部ファイル サーバの公開キーの取得

外部ファイル サーバ 公開キーを取得します。

始める前に

外部ファイル サーバのディレクトリのセットアップ（252 ページ）

手順

Step 1 ファイル サーバのパブリック キーを取得するには、次のように入力します。

```
$ ssh-keyscan -t rsa host
```

host はファイル サーバのホスト名、FQDN、または IP アドレスです。

警告
- ファイルサーバのパブリック キーをスプーフィングする「中間者攻撃」を防ぐには、**ssh-keyscan -t rsa** *host* コマンドで返されるパブリック キーの値が、ファイル サーバの実際のパブリック キーであることを確認する必要があります。
- ファイル サーバで、（このシステムでは `/etc/ssh/` の下にある）`ssh_host_rsa_key.pub` ファイルの場所に移動し、パブリック キー ファイルの内容と、**ssh-keyscan -t rsa** *host* コマンドで返されたパブリック キー値を比べて、ホスト以外の部分が一致することを確認してください（ファイル サーバの `ssh_host_rsa_key.pub` ファイルにはホストが存在しません）。

Step 2 `ssh_host_rsa_key.pub` ファイルの内容ではなく、**`ssh-keyscan -t rsa`** *`host`* コマンドの結果をコピーします。サーバのホスト名、FQDN、または IP アドレスから最後まで、必ずキー値全体をコピーしてください。

（注） ほとんどの場合、サーバのキーはホスト名または FQDN で始まりますが、IP アドレスで始まることもあります。

たとえば、次の内容をコピーします。

hostname ssh-rsa AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs...

...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ==

（... を追加）。

Step 3 **`ssh-keyscan -t rsa`** *`host`* コマンドの結果をテキスト ファイルに保存します。これは、「*IM and Presence Service* での外部ファイル サーバの展開」の手順でファイル サーバを設定するときに必要になります。

Step 4 作成した `authorized_keys` ファイルを開き、開いたままにしておきます。後に、IM and Presence Serviceでファイル サーバをプロビジョニングする際にこれが必要となります。

（注） 公開キーを取得できない場合は、外部ファイル サーバの公開キーおよび秘密キーのトラブルシューティング （260 ページ）で詳細なヘルプを参照してください。

次のタスク

IM and Presence Service での外部ファイル サーバのプロビジョニング （254 ページ）

IM and Presence Service での外部ファイル サーバのプロビジョニング

マネージド ファイル転送を有効にするクラスタ内の各ノードについて、1 つの外部ファイル サーバ インスタンスを設定する必要があります。

外部ファイル サーバ インスタンスは、外部ファイル サーバの物理インスタンスである必要はありません。ただし、ある 1 つのホスト名に関して、それぞれの外部ファイル サーバ インスタンス用に一意の外部ファイル サーバ ディレクトリ パスを指定する必要があります。同じノードから、すべての外部ファイル サーバ インスタンスを設定できます。

始める前に

外部ファイル サーバの公開キーの取得 （253 ページ）

外部ファイル サーバに関する以下の情報を取得します。

- ホスト名、FQDN、または IP アドレス
- 公開鍵
- ファイル ストレージ ディレクトリへのパス

- ユーザ名

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**メッセージング** > **外部サーバの設定** > **外部ファイル サーバ**を選択します。

Step 2 **[新規追加]** をクリックします。
[外部ファイルサーバ（External File Servers）] ウィンドウが表示されます。

Step 3 サーバの詳細を入力します。フィールドおよび設定オプションの詳細については、外部ファイル サーバのフィールド（255 ページ）を参照してください。

Step 4 **[保存（Save）]** をクリックします。

Step 5 マネージド ファイル転送が有効化されているクラスタ ノードごとに、個別の外部ファイル サーバ インスタンスを作成するまで、この手順を繰り返します。

次のタスク

Cisco XCP File Transfer Manager のアクティベーションの確認 （256 ページ）

外部ファイル サーバのフィールド

フィールド	説明
名前	ファイル サーバの名前を入力します。すぐに識別できるよう、サーバ名はできるだけ説明的な名前にしてください。 最大文字数は 128 文字です。使用できる文字は英数字、ダッシュ、および下線文字です。
ホスト/IP アドレス（Host/IP Address）	ファイル サーバのホスト名または IP アドレスを入力します。 （注） • [ホスト/IPアドレス（Host/IP Address）] フィールドに入力する値は、下記の [外部ファイルサーバパブリックキー（External File Server Public Key）] フィールドで指定するキーの先頭部分と一致する必要があります。 • この設定を変更した場合は、Cisco XCP Router サービスを再起動する必要があります。

フィールド	説明
外部ファイルサーバパブリックキー（External File Server Public Key）	ファイル サーバのパブリック キー（テキスト ファイルに保存するよう指示されたキー）を、このフィールドに貼り付けます。 キーを保存しなかった場合は、次のコマンドを実行してファイルサーバからそれを取得できます。 `$ ssh-keyscan -t rsa host`（ファイル サーバ上で）*host* は、ファイル サーバの IP アドレス、ホスト名、または FQDN です。 ホスト名、FQDN、または IP アドレスから始まって末尾まで、キーのテキスト全体をコピー/ペーストする必要があります。たとえば、次のようにコピーします。 extFileServer.cisco.com ssh-rsa AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs... ...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ== （... を追加）。 **重要** この値は必ず、[ホスト/IPアドレス（Host/IP Address）] フィールドに入力したホスト名、FQDN、またはIPアドレスで始まる必要があります。たとえば [ホスト/IPアドレス（Host/IP Address）] フィールドで extFileServer が使用されている場合は、このフィールドの先頭部分は extFileServer となり、その後に rsa キー全体が続きます。
外部ファイルサーバディレクトリ（External File Server Directory）	ファイル サーバ ディレクトリ階層の最上位のパス（例：`/opt/mftFileStore/node_1/`）。
ユーザ名	外部ファイル サーバ管理者のユーザ名。

Cisco XCP File Transfer Manager のアクティベーションの確認

マネージド ファイル転送が有効になっている各ノードで、Cisco XCP File Transfer Manager サービスが有効化されていなければなりません。

外部データベースおよび外部ファイルサーバーがすでに割り当てられており、さらにサービスがデータベースに接続してファイル サーバをマウントできる場合にのみ、このサービスが起動します。

始める前に

IM and Presence Service での外部ファイル サーバのプロビジョニング（254 ページ）

手順

Step 1 クラスタ内のいずれかのノードで [Cisco Unified IM and Presenceのサービスアビリティ（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。

Step 2 **[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。

Step 3 **サーバ**ドロップダウンから、マネージドファイル転送が有効になっているノードを選択して、**移動**をクリックします。

Step 4 **Cisco XCP File Transfer Manager** サービスの **アクティベーション ステータス** が **アクティブ済**であることを確認します。

Step 5 サービスが非アクティブ化されている場合は、**Cisco XCP File Transfer Manager** チェックボックスをオンにして、**保存**をクリックします。

Step 6 マネージドファイル転送が有効になっているすべてのクラスタ ノードで、この手順を繰り返します。

次のタスク

マネージド ファイル転送の有効化 （257 ページ）

マネージド ファイル転送の有効化

IM and Presence Serviceでのマネージド ファイル転送を有効にします。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**にログインし、**メッセージング** > **ファイル転送**を選択します。**ファイル転送** ウィンドウが開きます。

Step 2 ファイル転送設定エリアで、導入に応じて、**マネージド ファイル転送** あるいは **マネージド ピアツーピアファイル転送** を選択します。ファイル転送のオプション （258 ページ）を参照してください。

Step 3 [最大ファイルサイズ（Maximum File Size）] を入力します。0 を入力すると、最大サイズ（4 GB）が適用されます。

（注） この変更を有効にするには、Cisco XCP Router サービスを再起動する必要があります。

Step 4 [マネージドファイル転送の割り当て（Managed File Transfer Assignment）] エリアで、クラスタの各ノードに対して外部データベースと外部ファイル サーバを割り当てます。

a) 外部データベース：ドロップダウン リストから、外部データベースの名前を選択します。
b) 外部ファイル サーバ：ドロップダウン リストから、外部ファイル サーバの名前を選択します。

Step 5 [保存（Save）] をクリックします。

[保存（Save）] をクリックすると、それぞれの割り当てに対して [ノードパブリックキー（Node Public Key）] リンクが表示されます。

Step 6 マネージドファイル転送が有効になるクラスタ内の各ノードについて、ノードのパブリック キー全体を外部ファイル サーバの `authorized_keys` ファイルにコピーする必要があります。

a) ノードのパブリック キーを表示するには、[マネージドファイル転送の割り当て（Managed File Transfer Assignment）] エリアをスクロール ダウンして [ノードパブリックキー（Node Public Key）] リンクをクリックします。ノードの IP アドレス、ホスト名、FQDN を含めて、ダイアログボックスの内容全体をコピーします。

例：

```
ssh-rsa yc2EAAAABIwAAAQEAp2g+S2XDEzptN11S5h5nwVleKBnfG2pdW6KiLfzu/sFLegioIIqA8jBguNY/...
...5s+tusrtBBuciCkH5gfXwrsFS0O0AlfFvwnfq1xmKmIS9W2rf0Qp+A+G4MVpTxHgaonw== imp@imp_node
```

（... を追加）。

警告
- マネージドファイル転送機能が設定されいる場合、[ファイル転送タイプ（File Transfer Type）] が [無効（Disabled）] または [ピアツーピア（Peer-to-Peer）] に変更されると、マネージド ファイル転送のすべての設定が削除されます。
- 外部データベースおよびファイルサーバからノードが割り当て解除されると、ノードのキーは無効になります。

b) 外部ファイル サーバ上で、*mftuser* のホームディレクトリの下に作成した *~mftuser*/.ssh/authorized_keys ファイルがまだ開いていない場合は、これを開いて、（新しい行で）各ノードのパブリック キーを付加します。

（注） `authorized_keys` ファイルには、ファイル サーバに割り当てられている、マネージド ファイル転送が有効な各 IM and Presence Service ノードのパブリック キーが含まれる必要があります。

c) `authorized_keys` ファイルを保存して閉じます。

Step 7 （オプション）マネージド ファイル転送サービス パラメータを設定して、外部ファイル サーバのディスク領域に関する RTMT アラートが生成されるしきい値を定義します。

Step 8 マネージド ファイル転送が有効になっているすべてのノード上で、Cisco XCP Router サービスを再起動します。「Cisco XCP Router サービスの再起動」を参照してください。

次のタスク

外部サーバのステータスの確認 （259 ページ）

ファイル転送のオプション

次のいずれかのオプションを [ファイル転送] ウィンドウで設定することができます。

ファイル転送オプション	説明（**Description**）
Disabled	ファイル転送がクラスタで無効化されています。
ピアツーピア	1 対 1 のファイル転送は許可されますが、サーバではファイルのアーカイブや保存が行われません。グループ チャットのファイル転送はサポートされません。
マネージド ファイル転送	1 対 1 およびグループのファイル転送が許可されます。ファイル転送がデータベースのログに記録され、転送されたファイルはサーバに保存されます。クライアントがマネージドファイル転送をサポートしている必要もあります。そうでない場合、ファイル転送は許可されません。
マネージド ファイル転送およびピアツーピア ファイル転送	1 対 1 およびグループのファイル転送が許可されます。ファイル転送がデータベースのログに記録され、転送されたファイルはサーバに保存されます（ただしクライアントがマネージド ファイル転送をサポートする場合のみ）。クライアントがマネージドファイル転送をサポートしていない場合、このオプションはピアツーピア オプションと同等になります。

（注） マネージドファイル転送がノードで設定されていて、ファイル転送タイプを**無効**または**ピアツーピア**に変更した場合は、そのノードの外部データベースと外部ファイル サーバにマップされた設定が削除されることに注意してください。データベースとファイル サーバの設定は残りますが、そのノードでマネージドファイル転送を再び有効にする場合は、データベースとファイル サーバの再割り当てが必要になります。

アップグレード以前の設定により、IM and Presence Service リリース 10.5(2) 以降へのアップグレード後、**無効にする** あるいは **ピアツーピア** が選択されています。

外部サーバのステータスの確認

外部データベースの設定と外部ファイル サーバの設定に問題がないことを確認します。

始める前に

マネージド ファイル転送の有効化 （257 ページ）

手順

Step 1 外部データベースのステータスを確認するには：

a) **Cisco Unified CM IM and Presence 管理**で、**メッセージング** > **外部サーバの設定** > **外部データベース**を選択します。

b) [外部データベースのステータス（External Database Status）]エリアに示される情報を確認します。

Step 2 外部ファイルサーバーが割り当てられたことを確認するIM and Presence Service ノードで：

a) **Cisco Unified CM IM and Presence 管理**で、**メッセージング** > **外部サーバの設定** > **外部ファイル サーバ**を選択します。

b) 外部ファイルサーバーのステータス エリアに示される情報を確認して、接続に問題がないことを確認します。

外部ファイルサーバの公開キーおよび秘密キーのトラブルシューティング

サーバのプライベート/パブリック キー ペアが生成されるとき、プライベート キーは通常、`/etc/ssh/ssh_host_rsa_key` に書き込まれます。

パブリック キーは `/etc/ssh/ssh_host_rsa_key.pub`に書き込まれます。

これらのファイルがない場合は、以下の手順に従ってください。

手順

Step 1 次のコマンドを入力します。

```
$ ssh-keygen -t rsa -b 2048
```

Step 2 ファイル サーバのパブリック キーをコピーします。

ホスト名、FQDN、またはIP アドレスから、パブリック キーのテキストの文字列全体をコピーする必要があります（例：*hostname* ssh-rsa AAAAB3NzaC1yc...）。ほとんどのLinux 環境では、サーバのホスト名またはFQDN がキーに含まれています。

ヒント `$ ssh-keygen -t rsa -b 2048` コマンドの出力にホスト名が含まれていない場合は、代わりに `$ ssh-keyscan` *`hostname`* コマンドの出力を使用します。

Step 3 このファイル サーバを使用するように設定されている IM and Presence Service の各ノードについて、[外部ファイルサーバ設定（External File Server Configuration）] ウィンドウの [外部ファイルサーバパブリックキー（External File Server Public Key）] フィールドにパブリック キーを貼り付けてください。

重要 マネージドファイル転送機能には、パスワードを使用しないSSHを設定する必要があります。パスワードを使用しないSSHを設定する手順の詳細については、SSHDマニュアル ページを参照してください。

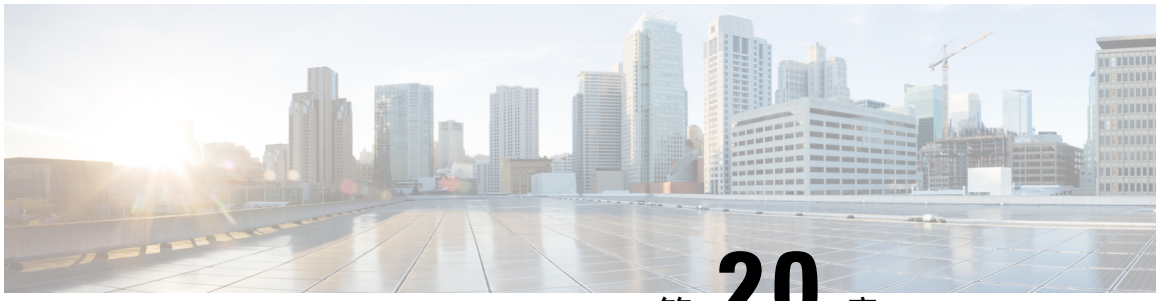
（注） パブリッシャ ノードからサブスクライバ ノードにステータスを確認するとき、および逆方向に確認するとき、「この外部ファイル サーバ用の診断テストは次から実行される場合があります（The diagnostics tests for this External File Server may be run from here.）」という情報メッセージが表示されます。

このログには、「-7」つまり外部ファイルサーバーが設定されていない他のノードのステータスを表示していることを示す、「ping」が表示されます。

パブリッシャーノードでは外部ファイルサーバを設定し、パブリッシャ ノードの公開キーは外部ファイルサーバの「Authorized_key」ファイルで共有されます。

マネージド ファイル転送の管理

マネージド ファイル転送を設定した後、この機能を継続的に管理する必要があります。たとえば、ファイル サーバとデータベースの拡張を管理するためにシステムを導入する必要があります。マネージド ファイル転送の管理の概要 （319 ページ）。



第 20 章

Multiple Device Messaging の設定

Multiple Device Messaging の概要

Multiple Device Messaging（MDM）により、現在サインインしているすべてのデバイス間で追跡される、1 対 1 のインスタント メッセージ（IM）交換が実現します。デスクトップ クライアントとモバイル デバイスを使用し、どちらも MDM が有効な場合、メッセージは両方のデバイスに送信されるか、または CC で送信されます。既読通知は、会話の参加中に両方のデバイスで継続的に同期されます。

MDM を使用すると、任意のデバイス間を移動しつつ、IM の会話を維持することができます。たとえば、デスクトップ コンピュータから IM 交換を開始した場合、デスクを離れた後でも、モバイル デバイスで会話を続けることができます。クライアントは、MDM が有効になっている場合に、ログインする必要があります。ログアウトしたクライアントには、送受信された IM および通知は表示されません。

MDM は、モバイル デバイスのバッテリを節約できる静音モードをサポートします。Jabber クライアントは、モバイル クライアントが使用されていないときは自動的に静音モードに切り替わります。静音モードはクライアントが再びアクティブになるとオフになります。

Multiple Device Messaging の要件

インスタントメッセージングを有効にする必要があります。詳細については、「グループチャットおよび常設チャットのタスク フロー（211 ページ）」を参照してください。

（注） Multiple Device Messaging を有効にする場合は、各ユーザが複数の Jabber クライアントを持つ可能性があるため、ユーザ数ではなくクライアント数に応じた展開にします。たとえば、ユーザ数が 25,000 人で、各ユーザが 2 台の Jabber クライアントを保持している場合、導入環境には 5 万ユーザのキャパシティが必要となります。

Multiple Device Messaging の設定

Multiple Device Messaging はデフォルトで有効になっています。機能を無効にしたり、無効にした後に再度オンにしたりするには、以下の手順を使用します。

手順

Step 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。

Step 2 [サーバ（Server）] ドロップダウン リストから、[IM and Presence サービス パブリッシャ（IM and Presence Service Publisher）] ノードを選択します。

Step 3 [サービス（Service）] ドロップダウン リストから、[Cisco XCP ルータ（アクティブ）（Cisco XCP Router (Active)）] を選択します。

Step 4 **Multi-Device Messagingの有効化** ドロップダウンリストから、**有効**（デフォルト値）あるいは **無効**のいずれかを選択します。

Step 5 **[保存（Save）]** をクリックします。

Step 6 Cisco XCP Router サービスを再起動します。

a) Cisco Unified IM and Presence Serviceability にログインして、**ツール > 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。

b) **サーバ** ドロップダウン リスト ボックスから IM and Presence パブリッシャ ノードを選択します。

c) [IM and Presenceサービス（IM and Presence Services）] の下で、[Cisco XCPルータ（Cisco XCP Router）] を選択し、[リスタート(Restart)] をクリックします

Multiple Device Messaging のフロー のユースケース

このフローでは、ユーザ（Alice）がラップトップとモバイル デバイスで MDM を有効化した際にメッセージと通知がどのように処理されるかについて説明しています。

1. Alice はラップトップ上で Jabber クライアントを開いており、モバイル デバイスでも Jabber を使用しています。
2. Alice は Bob からインスタント メッセージ（IM）を受け取ります。

   Alice のラップトップが通知を受信すると、新しいメッセージ インジケータが表示されます。モバイル デバイスには通知ではなく、新しいメッセージとして表示されます。

（注） IM は必ずすべての MDM 対応クライアントに一斉送信されます。通知はアクティブな Jabber クライアントにのみ表示されます。アクティブな Jabber クライアントがない場合は、すべての Jabber クライアントに通知が送信されます。

3. Alice は 20 分間 Bob とチャットしました。

   ラップトップでチャットする一方、モバイル デバイスでは新しいメッセージを受信し、既読として処理されます。モバイル デバイスには通知が送信されません。
4. Alice は 3 人目のユーザ（Colin）から 3 通のチャット メッセージを受信します。この際も Alice のデバイスはステップ 2 と同じように動作します。
5. Colin からのメッセージには応答せず、ラップトップを閉じます。帰路で Alice は Bob から別のメッセージを受信します。

   この状況では、ラップトップとモバイル デバイスの両方で新しいメッセージを受信し、通知を表示します。
6. Alice はモバイル デバイスを開き、Bob と Colin から送信された新しいメッセージを見つけます。これらのメッセージはラップトップにも送済みです。
7. Alice がモバイル デバイスでメッセージを読むと、メッセージはラップトップとモバイル デバイスの両方で既読になります。

Multiple Device Messaging における静音モードのユースケース

このフローでは、モバイル デバイス上で Multiple Device Messaging が静音モードを有効にする手順について説明します。

1. Alice は、ラップトップとモバイル デバイスで Jabber を使用しています。Bob からのメッセージを読み、ラップトップ上の Jabber から返信します。

2. モバイル デバイスで別のアプリケーションを使い始めます。ここで Jabber はバックグラウンドで動作し続けます。
3. Jabber がバックグラウンドで実行している間、静音モードは自動的に有効になります。
4. Bob が Alice に別のメッセージを送信します。Alice のモバイル デバイスでは Jabber が静音モードにあるため、メッセージは配信されません。Alice から Bob への応答メッセージはバッファとして保存されます。
5. メッセージのバッファリングは、次のトリガーイベントのいずれかが発生するまで続きます。
   - `<iq>` スタンザが受信される。
   - 他の Alice のデバイスでアクティブなクライアントがない場合に、`<message>` スタンザが受信される。

（注） アクティブなクライアントとは、過去 5 分間に、使用可能なプレゼンス ステータスまたはインスタント メッセージのいずれかを送信した最後のクライアントのことです。

   - バッファの制限に達した。
6. Alice がモバイル デバイスの Jabber に戻ると、再びアクティブになります。バッファとして保存された Bob のメッセージが配信され、Alice から閲覧可能になります。

Multiple Device Messaging のインタラクションと制限

次の表では、Multiple Device Messaging（MDM）機能との機能の相互作用および制限をまとめています。

表 *25 : Multiple Device Messaging* のインタラクションと制限

機能	連携動作または制限事項
Cisco Jabber クライアント	MDM はバージョン 11.7 以降のすべての Jabber クライアントによりサポートされます。
グループ チャット	グループチャットは、どのデバイスからサインインした MDM ユーザーでも利用可能です。
メッセージ アーカイバ	MDM は、メッセージ アーカイバ機能と互換性があります。
マネージド ファイル転送	ファイル転送は、どのデバイスからサインインした MDM ユーザーでも利用可能です。

機能	連携動作または制限事項
Expressway経由でのモバイルおよびリモートアクセス	Cisco Expressway 経由で IM and Presence Service に接続するモバイルおよびリモートアクセスの場合、MDM を使用するには、少なくとも Expressway X8.8 が実行されていなければなりません。
Server Recovery Manager	フェールオーバーが発生した場合、Multiple Device Messaging 機能により、IM and Presence サービスでサーバ回復に遅延が発生します。Multiple Device Messaging が設定されているシステムでサーバのフェールオーバーが発生すると、フェールオーバーの時間は通常、**Cisco Server Recovery Manager** サービス パラメータで指定された時間の 2 倍になります。
サードパーティ製クライアント	MDM は、この機能をサポートしていないサードパーティクライアントと互換性があります。

複数のデバイスのメッセージングのカウンタ

Multiple Device Messaging（MDM）は、Cisco XCP MDM カウンタ グループから次のカウンタを使用します。

カウンタ名	説明
MDMSessions	MDM が有効な現在のセッション数。
MDMSilentModeSessions	サイレント モードにおける現在のセッション数。
MDMQuietModeSessions	静音モードにおける現在のセッション数。
MDMBufferFlushes	MDM バッファ フラッシュの合計数。
MDMBufferFlushesLimitReached	バッファ サイズ全体の上限に到達したことで発生した MDM バッファ フラッシュの合計数。
MDMBufferFlushPacketCount	最後のタイムスライスでフラッシュされたパケットの数。
MDMBufferAvgQueuedTime	MDM バッファがフラッシュされるまでの平均時間（秒）。

デバイス容量のモニタリング

複数のデバイスメッセージング(MDM)を有効にすると、複数のデバイスからログインした各ユーザは、IM and Presence サーバのトラフィック負荷を増加させることになります。ログインしているアクティブなユーザの数が特定の制限に達すると、リソース不足(メモリ消費量、CPU使用率)、および予期しないパフォーマンスの問題と障害が発生します。

これらの問題に対処するには、デバイスキャパシティモニタリング機能が役立ちます。この機能は、ノードで作成されたセッション数のモニタリングを支援する追加のカウンタを実装します。

IM&P ノードでは、次の Jabber Session Manager (JSM) セッションが作成されます。

- 構成された JSM セッション: ユーザがノードに割り当てられると作成されます。
- アクティブな JSM セッション

  -オンプレミスのユーザログイン。

  – オフプレミスのユーザ ログイン。

- ファントム JSM セッション: HA フェールオーバーの使用例を処理するプッシュ対応ユーザ用。
- Spark Interop JSM session: ハイブリッドユーザ用。

JSM セッションをモニタするために、次のカウンタが導入されています。

- **JsmClientSessionsActive**
- **JsmPhantomSessionsActive**
- **JsmHybridSessionsActive**

さらに、jsm セッションカウンタと OVA サイズに基づいて計算される JSM しきい値制限をモニタするために、新しいカウンタ**Jsmsessionsexceedsthreshold**が導入されました。

このカウンタのしきい値制限が10分間のデフォルト値の80% を超えると、システムはリアルタイムモニタリングツール (RTMT) で「**Jsmsessionsexceedsthreshold**」アラートを生成します。

RTMT を使用したアラート値の設定

この手順を使用して、RTMT を使用して**Jsmsessionsexceedsthreshold**アラート値を設定できます。

手順

Step 1 **リアルタイムモニタリングツール (RTMT)**にログインし、 **System** > **Tools** > **Alert Central**を選択します。

Step 2 [**IM and Presence**] をクリックし、[**Jsmsessionsexceedsthreshold** Alert name] を選択します。

Step 3 [**Jsmsessionsexceedsthreshold**] を右クリックし、[**Set Alert/Properties**] を選択します。

Step 4 アラートを有効にするには、[アラートの有効化（Enable Alert）] チェックボックスをオンにします。

Step 5 JSMセッションしきい値の超過値のパーセンテージ制限を設定します。デフォルトでは、値は80%です。

Step 6 [保存（Save）] をクリックします。

Step 7 アラートの頻度とスケジュールを設定します。デフォルトでは、アラートは10分ごとにトリガーされます。

Step 8 [次へ（Next）] をクリックします。

Step 9 [保存（Save）] をクリックします。

ノードごとの JSM セッションのサポート

次の表に、テストに基づいてノードごとにサポート可能な JSM セッションの合計数を示します。

OVA サイズ	JSM セッション数が OVA キャパシティの1.5 倍
5K OVA	7.5K
15,000 OVA	22.5 k
25K OVA	37.5 k

（注） ハイアベイラビリティが有効になっており、両方のノードがアクティブ-アクティブコンフィギュレーションの場合、次のようになります。

1. ノードごとにサポート可能な JSM セッションの合計数は、上記のキャパシティの50% になります。カスタムアラームには、ノードごとにのみ設定できる制限があるためです。
2. HA 設定に基づいて、 **Jsmsessionsexceedsthreshold**カウンタの値を変更する必要があります。

推奨する行動：

カスタムアラートが発生した場合は、特定のノードの RTMT ツールからメモリと CPU 使用率のカウンタを確認します。メモリと CPU 使用率のカウンタの値がしきい値制限を超える場合は、IM&P ノード間でユーザのロードバランスを行うことをお勧めします。現在、IM&P には、ノード間でユーザを自動的にロードバランシングするメカニズムがありません。

デバイス キャパシティ モニタリングのユーザ セッション レポート

ユーザセッションレポートを表示するには、次の手順を使用します。このレポートでは、クラスタ、サブクラスタ、およびノードレベルの複数のデバイスからログインしているアクティブユーザの詳細を確認できます。

手順

Step 1 **Cisco Unified IM and Presence Reporting** にログインします。

Step 2 **[システムレポート（System Reports）] > [IM and Presence ユーザセッションレポート（IM and Presence User Sessions Report）]** を選択します。

Step 3 現在の時刻のユーザセッションレポートを生成するには、[レポート (reports)] ウィンドウで **[レポートの生成 (Generate Report)]** (棒グラフ) アイコンを選択します。

Step 4 [OK] をクリックします。

Step 5 列**レポート名**の下で、 **IM and Presence ユーザセッションレポート**をクリックします。

（注）
- このレポートの生成には約2分以上かかる場合があります。
- このレポートには、プレゼンス冗長グループ、ノード名、1 つ以上のデバイスからログインしているユーザの数、クラスタ、サブクラスタ、およびノードレベルのセッションの合計数が、レポートの生成日時と共に表示されます。

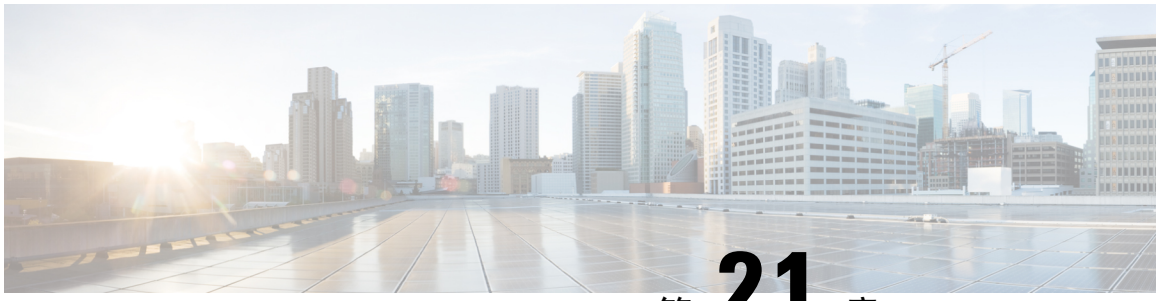
Step 6 [レポート (Reports)] ウィンドウの右側にある **[ダウンロード (download)]** (緑色の矢印) アイコンをクリックして、クラスタ、サブクラスタ、およびノードレベルのユーザセッションレポートを CSV 形式でダウンロードします。

Step 7 特定のノードの詳細なユーザベースのレポートを生成するに**は、1つ以上のデバイスからログイン**しているユーザの列数にリストされている値をクリックします。

Step 8 [レポート (Reports)] ウィンドウの右側にある **[ダウンロード (download)]** (緑色の矢印) アイコンをクリックして、ノードごとの詳細なユーザレベル情報を CSV 形式でダウンロードします。

（注） **[セッション数（Number of sessions）]** 列の上にマウスカーソルを合わせると、**[デバイスタイプ（device type）]** ツールチップに、ログインに使用したデバイスのタイプが表示されます。

たとえば、デバイスタイプはデスクトップ、iPad、iPhone になる可能性があります。



第 21 章

エンタープライズ グループの設定

エンタープライズ グループの概要

エンタープライズ グループを設定すると、Cisco Unified Communications Manager は、データベースを外部 LDAP ディレクトリと同期するときにユーザ グループを含めます。Cisco Unified CM の管理では、[ユーザグループ（User Groups）] ウィンドウで同期されたグループを表示できます。

この機能は、管理者が以下を行う場合にも役立ちます。

- 機能のコメント セット（たとえば、セールス チームやアカウンティング チーム）と同様の特性を持つユーザのプロビジョニング。
- 特定のグループのすべてのユーザを対象にしたメッセージの送信。
- 特定のグループのすべてのメンバーへの統一されたアクセスの設定

この機能は、Cisco Jabber ユーザが共通特性を共有するユーザの連絡先リストをすばやく作成するのにも役立ちます。Cisco Jabber ユーザは、外部 LDAP ディレクトリでユーザ グループを検索し、それらを連絡先リストに追加できます。たとえば、Jabber ユーザは外部 LDAP ディレクトリを検索してセールス グループを連絡先リストに追加することで、すべてのセールス チーム メンバーを連絡先リストに追加することができます。グループが外部ディレクトリで更新されると、ユーザの連絡先リストは自動的に更新されます。

エンタープライズ グループは、Windows 上の Microsoft Active Directory で外部 LDAP ディレクトリとしてサポートされています。

（注） エンタープライズ グループ機能を無効にすると、Cisco Jabberユーザは、エンタープライズ グループを検索したり、自分の連絡先リストに追加済みのグループを表示したりできません。ユーザがログイン中にその機能を無効にすると、そのユーザがログアウトするまでグループは表示されます。ユーザが再度ログインすると、グループは表示されません。

セキュリティ グループ

セキュリティ グループは、エンタープライズ グループのサブ機能です。Cisco Jabber ユーザは、セキュリティ グループを検索して、自分の連絡先リストに追加できます。この機能を設定するには、管理者がカスタマイズした LDAP フィルタを設定し、設定された LDAP ディレクトリの同期に適用する必要があります。セキュリティ グループは、Microsoft Active Directory でのみサポートされています。

許可されるエントリの最大数

エンタープライズ グループを設定するときは、グループを処理する連絡先リストの最大値を設定してください。

- 連絡先リストで許可されるエントリの最大数は、連絡先リストのエントリ数と連絡先リストに追加されているグループのエントリ数の合計です。
- 連絡先リスト内の最大エントリ数 = 連絡先リスト内のエントリ数 + グループ内のエントリ数
- エンタープライズ グループ機能が有効になっているときに、連絡先リスト内のエントリ数が許容最大エントリ数よりも少ない場合、Cisco Jabber ユーザはグループを連絡先リストに追加できます。この機能が無効になっているときに許容最大エントリ数を超えていた場合、この機能が有効にされるまでユーザは制限を受けません。この機能が有効にされた後もユーザがログインし続けた場合、エラー メッセージは表示されません。そのユーザがログアウトした後に再度ログインしたとき、超過したエントリをクリアするようにユーザに求めるエラー メッセージが表示されます。

エンタープライズ グループの前提条件

この機能は、以下の条件で LDAP ディレクトリの同期スケジュールを設定していることを前提としています。LDAP ディレクトリ同期を設定する方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Import Users from LDAP Directory」の章を参照してください。

- Cisco DirSync サービスが有効になっている必要があります。
- LDAP ディレクトリ同期には、ユーザとグループの両方が含まれている必要があります。
- 通常の LDAP ディレクトリ同期は、[LDAPディレクトリ同期スケジュール(LDAP Directory Synchronization Schedule)] で設定されているとおりにスケジュールされている必要があります。

サポートされる LDAP ディレクトリ

エンタープライズ グループでは、Microsoft Active Directory のみがサポートされています。

LDAP ディレクトリ	エンタープライズ グループのサポート
Microsoft Active Directory	エンタープライズグループとセキュリティグループの両方がサポートされています。
OpenLDAP	Windows 上の OpenLDAP では、次のサポートがあります。 • `GroupOfNames` オブジェクト クラスのみがサポートされています。 • セキュリティ グループは、OpenLDAP でサポートされていません。 • 最小バージョンは 2.4.42 です。 • Linux での OpenLDAP はサポートされていません。
他の LDAP ディレクトリ	未サポート

エンタープライズ グループの設定タスク フロー

エンタープライズ グループ機能を設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
Step 1	LDAPディレクトリからのグループ同期の確認 （274 ページ）	LDAP ディレクトリの同期にユーザとグループの両方が含まれていることを確認します。
Step 2	エンタープライズ グループの有効化（274 ページ）	Cisco Jabber ユーザが Microsoft Active Directory のエンタープライズ グループを検索して自分の連絡先リストに追加できるようにするには、次のタスクを実行します。
Step 3	OpenLDAP 設定ファイルの更新（275 ページ）	（OpenLDAP のみ）Windows の OpenLDAP ディレクトリにある `slapd.conf` 設定ファイルを編集します。
Step 4	セキュリティ グループの有効化（275 ページ）	（任意）Cisco Jabber ユーザがセキュリティ グループを検索して自分の連絡先リストに

	コマンドまたはアクション	目的
		追加できるようにするには、次のタスクフローを完了します。
Step 5	ユーザ グループの表示 （278 ページ）	（オプション）Cisco Unified Communications Managerデータベースと同期する エンタープライズ グループおよびセキュリティ グループを表示します。

LDAP ディレクトリからのグループ同期の確認

LDAP ディレクトリ同期にユーザとグループが含まれていることを確認するには、次の手順を使用します。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[サーバ（Server）] > [LDAP] > [LDAP ディレクトリ（LDAP Directory）]**。

Step 2 [検索（Find）] をクリックし、エンタープライズ グループを同期する LDAP ディレクトリを選択します。

Step 3 [同期（Synchronize）] フィールドで [ユーザとグループ（Users and Groups）] が選択されていることを確認します。

Step 4 [LDAPディレクトリの設定（LDAP Directory configuration）] ウィンドウの残りのフィールドに入力します。フィールドとその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。

Step 5 [保存（Save）] をクリックします。

エンタープライズ グループの有効化

LDAP ディレクトリ同期にエンタープライズ グループを含めるようにシステムを設定します。

手順

Step 1 Cisco Unified CM の管理から、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

Step 2 [ユーザ管理パラメータ（User Management Parameters）] で、[Cisco IM and Presenceでのディレクトリグループの操作（Directory Group Operations on Cisco IM and Presence）] パラメータを [有効（Enabled）] に設定します。

Step 3 [プレゼンス情報を許可するためにサイズ設定された最大エンタープライズグループ（Maximum Enterprise Group Sized to allow Presence Information）] パラメータの値を入力します。許可される範囲は 1 ～ 200 ユーザーで、デフォルト値は 100 ユーザーです。

Step 4 **[エンタープライズグループの同期モード（Syncing Mode for Enterprise Groups）]** ドロップダウンリストから、定期的に実行する LDAP 同期を **[なし（None）]**、**[差分同期（Differential Sync）]**、**[完全同期（Full Sync）]** から選択して設定します。

（注） これらのフィールドの構成の詳細については、エンタープライズ パラメータのヘルプを参照してください。

Step 5 [保存（Save）] をクリックします。

OpenLDAP 設定ファイルの更新

Windows で OpenLDAP を介してエンタープライズ グループを設定する場合は、OpenLDAP ディレクトリの `slapd.conf` ファイルを更新する必要があります。

手順

Step 1 Windows の OpenLDAP ファイル ディレクトリで、`slapd.conf` ファイルを参照します。

Step 2 テキスト エディタでこのファイルを開きます。

Step 3 ファイルに次のテキストを追加します。

```
moduleload memberof.la
overlay memberof
memberof-group-oc groupOfNames
memberof-member-ad member
memberof-memberof-ad memberof
memberof-refint TRUE
cachesize 160000
```

Step 4 ファイルを保存します。

Step 5 OpenLDAP ディレクトリを再起動します。

セキュリティ グループの有効化

Cisco Jabber ユーザがセキュリティ グループを自分の連絡先リストに追加できるようにする場合は、以下のオプションのタスクを実行して、セキュリティ グループを LDAP ディレクトリ同期に追加します。

（注） セキュリティ グループの同期は、Microsoft Active Directory からのみ実行できます。

（注） 最初の同期がすでに発生した Cisco Unified Communications Manager では、LDAP ディレクトリの既存の構成に新しい設定を追加できません。

手順

	コマンドまたはアクション	目的
Step 1	セキュリティ グループ フィルタの作成（276 ページ）	ディレクトリ グループとセキュリティ グループの両方をフィルタ処理する LDAP フィルタを作成します。
Step 2	LDAP ディレクトリからのセキュリティ グループの同期化（276 ページ）	新しい LDAP フィルタを LDAP ディレクトリ同期に追加します。
Step 3	Cisco Jabber のセキュリティ グループの構成（277 ページ）	既存のサービスプロファイルを更新して、そのサービス プロファイルに関連付けられた Cisco Jabber ユーザに、セキュリティ グループを検索および追加するためのアクセス権が付与されるようにします。

セキュリティ グループ フィルタの作成

セキュリティ グループをフィルタリングする LDAP フィルタを作成します。

手順

Step 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **システム** > **LDAP** > **ldap フィルタ**。

Step 2 **[新規追加]** をクリックします。

Step 3 [Filter name（フィルタ名）] ボックスに一意の名前を入力します（例：「`syncSecurityGroups`」）。

Step 4 以下を入力します：Filter: (&(objectClass=group)(CN=*))

Step 5 [保存（Save）] をクリックします。

LDAP ディレクトリからのセキュリティ グループの同期化

LDAP ディレクトリ同期にセキュリティ グループ フィルタを追加し、同期を完了します。

（注） 最初の LDAP 同期がすでに発生している場合、Cisco Unified Communications Manager では、LDAP ディレクトリの既存の構成に新しい設定を追加できません。

（注） LDAPディレクトリ同期を新しく設定する方法の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Configure End Users」の項目を参照してください。

始める前に

セキュリティ グループ フィルタの作成 （276 ページ）

手順

Step 1 Cisco Unified CM の管理で、**[System（システム）] > [LDAP（LADP）] > [LDAP Directory（LDAP ディレクトリ)]** を選択します。

Step 2 次のいずれかを実行します。

- [新規追加（Add New）] をクリックして、新しい LDAP ディレクトリを作成します。
- [検索（Find）] をクリックして、同期されるセキュリティ グループから LDAP ディレクトリを選択します。

Step 3 [**グループの LDAP カスタム フィルタ（LDAP Custom Filter for Groups**）] ドロップダウン リストから、作成したセキュリティ グループ フィルタを選択します。

Step 4 **[保存（Save）]** をクリックします。

Step 5 **[LDAP ディレクトリ設定（LDAP Directory Configuration）]** ウィンドウのその他のフィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。

Step 6 [完全同期を今すぐ実施（Perform Full Sync Now）] をクリックして、すぐに同期します。それ以外の場合、セキュリティ グループは、スケジュール設定された次回の LDAP 同期が発生した時点で同期されます。

Cisco Jabber のセキュリティ グループの構成

既存のサービスプロファイルを更新して、そのサービスプロファイルに関連付けられている Cisco Jabber ユーザが、LDAP ディレクトリからセキュリティ グループを自分の連絡先リストに追加できるようにします。

（注） 新しいサービス プロファイルを設定して、Cisco Jabber ユーザに割り当てる方法については、『*Cisco Unified Communications Manager* システム構成ガイド』の「サービス プロファイルを構成する」の章を参照してください。

始める前に

LDAP ディレクトリからのセキュリティ グループの同期化 （276 ページ）

手順

Step 1 [サービス プロファイルの構成（Service Profile Configuration）] ウィンドウで、残りのフィールドを入力します。フィールドとその設定のヘルプは、オンライン ヘルプを参照してください。

Step 2 [検索（Find）] をクリックして、Jabber ユーザが使用するサービス プロファイルを選択します。

Step 3 [ディレクトリ プロファイル（Directory Profile）] の下で、[Jabber によるセキュリティ グループの検索と追加を許可する（Allow Jabber to Search and Add Security Groups）] チェック ボックスをオンにします。

Step 4 [保存（Save）] をクリックします。
これで、このサービス プロファイルに関連付けられている Cisco Jabber ユーザが、セキュリティ グループを検索および追加できるようになります。

Step 5 Cisco Jabber ユーザが使用するすべてのサービス プロファイルについて、この手順を繰り返します。

ユーザ グループの表示

Cisco Unified Communications Manager データベースと同期する エンタープライズ グループとセキュリティ グループを表示するには、次の手順を実行します。

手順

Step 1 Cisco Unified CM の管理で、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ユーザ グループ（User Group）]** の順に選択します。
[ユーザ グループの検索/一覧表示（Find and List User Group）] ウィンドウが表示されます。

Step 2 検索条件を入力して [検索（Find）] をクリックします。
検索条件に一致するユーザ グループのリストが表示されます。

Step 3 あるユーザ グループに属しているユーザのリストを表示するには、そのユーザ グループをクリックします。
[ユーザ グループの設定（User Group Configuration）] ウィンドウが表示されます。

Step 4 検索条件を入力して [検索（Find）] をクリックします。
検索条件に一致するユーザのリストが表示されます。

リスト内のユーザをクリックすると、[エンド ユーザの設定（End User Configuration）] ウィンドウが表示されます。

次のタスク

（省略可） セキュリティ グループの有効化 （275 ページ）

エンタープライス グループの導入モデル（Active Directory）

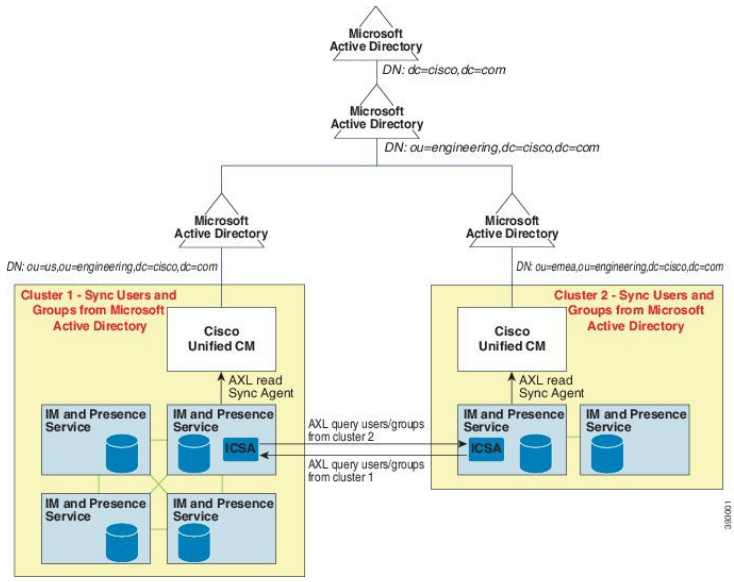
エンタープライズ グループ機能は、Active Directory 用に次の 2 つの導入オプションを提供します。

重要 Cisco Intercluster Sync Agent サービス経由でデータを同期する前に、クラスタ 1 とクラスタ 2 に、UserGroup レコード、UserGroupMember レコード、UserGroupWatcherList レコードの一意のセットが含まれていることを確認します。両方のクラスタにレコードの一意のセットが含まれている場合、同期後には両方のクラスタにすべてのレコードのスーパー セットが含められています。

エンタープライズ グループ導入モデル 1

この導入モデルでは、クラスタ 1 とクラスタ 2 が Microsoft Active Directory からの異なるユーザとグループのサブセットを同期します。Cisco Intercluster Sync Agent サービスは、データをクラスタ 2 からクラスタ 1 に複製して、ユーザとグループの完全なデータベースを作成します。

図 *8:* エンタープライズ グループ導入モデル *1*



エンタープライズ グループ導入モデル 2

この導入モデルでは、クラスタ 1 が Microsoft Active Directory からのすべてのユーザとグループを同期します。クラスタ 2 は、Microsoft Active Directory からのユーザのみを同期します。Cisco Intercluster Sync Agent サービスは、グループ情報をクラスタ 1 からクラスタ 2 に複製します。

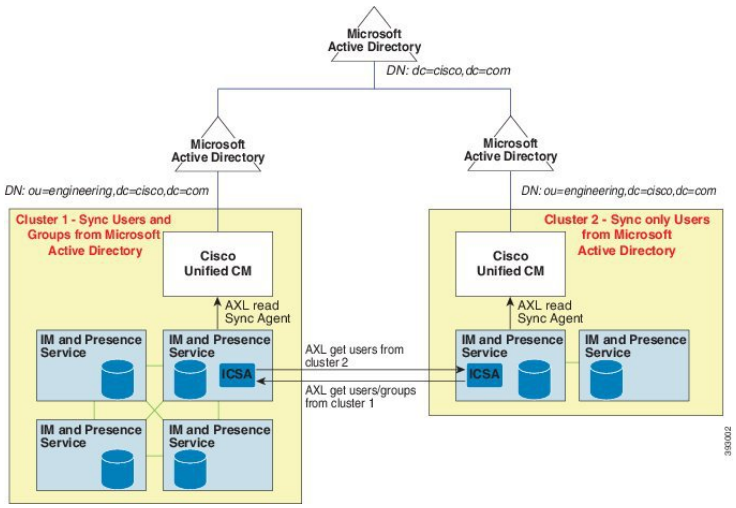
⚠

注意 この導入モデルを使用する場合は、1 つのクラスタ内のグループ データだけが同期されていることを確認します。そうでない場合は、エンタープライズ グループ機能が想定どおりに機能しません。

[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > **[プレゼンス（Presence）]** > **[クラスタ間設定（Inter-Clustering）]** ウィンドウで設定を確認できます。

クラスタ間ピア テーブルで [エンタープライズ グループ LDAP 設定（Enterprise Groups LDAP Configuration）] パラメータのステータスを確認します。[矛盾は見つかりませんでした（No conflict found）] は、ピア間に設定ミスがないことを意味します。矛盾が見つかった場合は、[エンタープライズ グループの矛盾（Enterprise GroupConflicts）] リンクをクリックして、表示された [詳細（details）] ボタンをクリックします。これにより、レポート ウィンドウが開いて、詳細なレポートが表示されます。

図 *9*：エンタープライズ グループ導入モデル *2*



エンタープライズ グループの制限事項

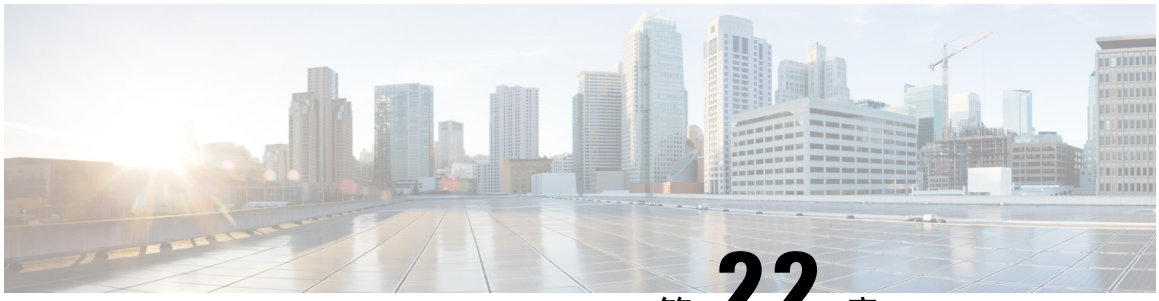
表 *26 :* エンタープライズ グループの制限事項

制限事項	説明（**Description**）
全員をブロック	Cisco Jabber ユーザが Cisco Jabber ポリシー設定から [全員をブロック（Block everyone）] 機能を有効にすると、ブロック機能により、他の Jabber ユーザは IM and Presence を表示したり、ブロックするユーザと IM and Presence を交換したりできなくなります。ただしブロックするユーザの連絡先リストに連絡先として登録されている場合を除きます。 たとえば、Cisco Jabber ユーザ（Andy）が Jabber の個人設定で [全員をブロック（Block everyone）] を有効にしたとします。Andy の個人用連絡先リストに含まれている Jabber ユーザと含まれていない Jabber ユーザに対して Andy のブロックがどのように影響するかを以下に説明します。Andy は、ブロックの他に、次のような個人用連絡先リストを持っています。 • Bob が含まれている：Bob は Andy の個人用連絡先リストに含まれているので、ブロックに関わらず、IM を送信し、Andy のプレゼンスを確認できます。 • Carol が除外されている：ブロックに基づき Carol は Andy のプレゼンスを確認できず、IM を送信できません。 • Deborah は個人連絡先から除外されています。ただし Deborah は、Andy が連絡先としてリストに含めたエンタープライズ グループのメンバーです。ブロック機能により、Deborah は Andy のプレゼンスの確認も Andy への IM 送信も実行できません。 Deborah は Andy の連絡先リストのエンタープライズ グループのメンバーであるにもかかわらず、Andy のプレゼンスの確認や Andy への IM の送信がブロックされる点に注意してください。エンタープライズ グループの連絡先の動作の詳細については、CSCvg48001 を参照してください。

制限事項	説明（**Description**）
10.x クラスタとのクラスタ間ピアリング	エンタープライズ グループは、リリース 11.0(1) 以降でサポートされます。 同期されたグループに 10.x クラスタ間ピアからのグループ メンバーが含まれている場合、より高いクラスタ上のユーザは 10.x クラスタからの同期されたメンバーのプレゼンスを確認できません。これは、エンタープライズ グループの同期用に 11.0(1) で導入されたデータベース更新が原因です。この更新は 10.x リリースの一部ではありません。 より高いクラスタをホームにしているユーザが 10.x クラスタをホームにしているグループ メンバーのプレゼンスを確認できることを保証するには、より高いクラスタ上のユーザが自分の連絡先リストに 10.x ユーザを手動で追加する必要があります。手動で追加されたユーザに関するプレゼンスの問題は存在しません。
複数レベルのグループ分け	複数レベルのグループ分けは、グループ同期に対して許可されません。
グループ専用同期	ユーザ グループとユーザが同じ検索ベース内に存在する場合、グループ専用同期は許容されません。代わりに、ユーザ グループとユーザが同期されます。
ユーザ グループの最大数	Microsoft Active Directory サーバから Unified Communications Manager データベースに最大 15000 のユーザ グループを同期できます。 各ユーザ グループには 1 ～ 200 人のユーザを含めることができます。 **[Cisco Unified CM IM and Presence Administration]** > **[システム（System）]** > **[サービス パラメータ（Service Parameters）]** ウィンドウで、正確な数を設定できます。 データベース内のユーザ アカウントの最大数は 160,000 を超えることはできません。
ユーザ グループの移行	ユーザ グループを組織単位間で移動する場合は、元の単位に対して完全同期を実行してから、新しい単位に対して完全同期を実行する必要があります。
ローカル グループ	ローカル グループはサポートされません。Microsoft Active Directory から同期されたグループのみがサポートされます。
IM and Presence Service ノードに割り当てられていないグループ メンバー	IM and Presence Service ノードに割り当てられていないグループ メンバーは、プレゼンス バブルが灰色表示されて連絡先リストに表示されます。ただし、これらのメンバーは、連絡先リストで許可されるユーザの最大数を計算する際に考慮されます。

制限事項	説明（**Description**）
Microsoft Office Communications Server からの移行	Microsoft Office Communications Server からの移行中は、ユーザが IM and Presence Service ノードに完全に移行されるまで、グループ エンタープライズ機能がサポートされません。
LDAP 同期	同期の進行中に、[LDAPディレクトリの設定（LDAP Directory Configuration）] ウィンドウで同期オプションを変更しても、既存の同期は影響を受けません。たとえば、同期の進行中に同期オプションを [ユーザとグループ（Users and Groups）] から [ユーザのみ（Users Only）] に変更しても、ユーザとグループの同期はそのまま継続されます。
エッジ経由のグループ検索機能	エッジ経由のグループ検索機能は、このリリースで提供されますが、完全にテストされているわけではありません。そのため、エッジ経由のグループ検索のフル サポートは保証できません。フル サポートは今後のリリースで提供される予定です。
Cisco Intercluster Sync Agent サービスの定期同期	外部 LDAP ディレクトリでグループ名またはグループ メンバー名を更新すると、定期 Cisco Intercluster Sync Agent サービス同期の後でしか Cisco Jabber 連絡先リストが更新されません。通常、Cisco Intercluster Sync Agent サービスの同期は 30 分ごとに実行されます。
LDAP 設定内の別々の同期アグリーメント経由のユーザとユーザ グループの同期	ユーザとユーザ グループが同じ同期アグリーメントの一部として Cisco Unified Communications Manager データベースに同期されている場合は、同期後に、Cisco Unified Communications Manager データベースで、想定されているようにユーザとグループの関連付けが更新されます。ただし、ユーザとユーザ グループが別々の同期アグリーメントの一部として同期されている場合は、最初の同期後、ユーザとグループはデータベースで関連付けされないことがあります。データベース内のユーザとグループの関連付けは、同期アグリーメントが処理される順序によって異なります。ユーザがグループより前に同期された場合は、データベース内でグループを関連付けに使用できない可能性があります。その場合は、グループとの同期アグリーメントがユーザとの同期アグリーメントより前にスケジュールされるようにします。そうでない場合は、グループをデータベースに同期した後、ユーザは次の手動同期または定期的に同期タイプを設定してユーザとグループとして同期した後にグループに関連付けられます。契約の同期タイプがユーザとグループとして設定されている場合にのみ、ユーザおよび対応するグループ情報がマップされます。 。

制限事項	説明（**Description**）
エンタープライズグループの検証済 OVA 情報	**検証 シナリオ** 2 つのクラスタを持つクラスタ間の導入では、クラスタ A とクラスタ B が使用されています。 クラスタ A は、Active Directory から同期される 160 k ユーザの IM and Presence Service で 15K OVA および 15K ユーザが有効になっています。15K OVA クラスタでは、ユーザあたりのエンタープライズグループの検証され、サポートされる平均数は 13 のエンタープライズ グループです。 クラスタ B では、Active Directory から同期される 160 k ユーザの IM and Presence Service で 25K OVA および 25K ユーザが有効になっています。25K OVA クラスタでは、ユーザあたりのエンタープライズグループの検証され、サポートされる平均数は 8 のエンタープライズ グループです。 名簿に記載されているユーザの個人連絡先と、ユーザの名簿に含まれるエンタープライズグループからの連絡先の、検証済およびサポートされる合計は、200 以下です。 （注） 2 つ以上のクラスタがある環境では、これらの数量はサポートされていません。
連絡先リストのエクスポート	**[一括管理（Bulk Administration）] > [連絡先リスト（Contact List）] > [連絡先リストのエクスポート（Export Contact List）]** を使用してユーザの連絡先リストをエクスポートすると、連絡先リストの CSV ファイルには、Jabber クライアントにあるエンタープライズグループの詳細が含まれません。



第 22 章

ブランディングのカスタマイズ

ブランディングの概要

ブランディング機能を使用すると、IM and Presence サービスのカスタマイズされたブランディングを適用できます。ブランディングのカスタマイズは、Cisco Unified CM IM and Presence 管理のログインおよび設定ウィンドウに表示されます。追加または変更できる項目には次のものがあります。

- 企業ロゴ
- 背景色
- 枠線色
- フォントの色

ブランディングの前提条件

指定されたフォルダ構造とファイルを含むブランディング zip ファイルを作成する必要があります。詳細については、「ブランディング ファイルの要件 （287 ページ）」を参照してください。

ブランディングの有効化

IM and Presence サービスクラスタのブランディングのカスタマイズを有効にするには、次の手順を使用します。SAML SSO が有効になっている場合でも、ブランディングの更新が表示されます。

（注） ブランディングを有効にするには、特権レベル 4 のアクセス権を持つプライマリ管理者アカウントを使用する必要があります。これは、インストール時に作成されるメインの管理者アカウントです。

（注） GUI と CLI のいずれか 1 つだけを使用して、ブランド化を有効にし、無効にするようにしてください。たとえば、GUI インターフェースを使用してブランド化を有効にする場合、GUI インターフェース自体を使用してブランド化を無効にする必要があります。そうしないと、正しく機能しません。

始める前に

IM and Presence サービスがアクセスできる場所に、IM およびプレゼンスのカスタマイズを使用してブランディングファイルを保存します。

手順

Step 1 Cisco Unified IM and Presence OS の管理にログインします。

Step 2 **[ソフトウェアアップグレード（Software Upgrades）] > [ブランディング（Branding）]** を選択します。

Step 3 リモート サーバを**参照**し、`branding.zip` ファイルを選択します。

Step 4 [ファイルのアップロード（Upload File）] をクリックします。

Step 5 [ブランディングの有効化（Enable Branding）] をクリックします。

（注） また、**utils branding enable** CLI コマンドを実行して、ブランディングを有効にすることもできます。

Step 6 変更内容を表示するには、ブラウザを更新します。

Step 7 すべての IM and Presence サービスのクラスタ ノードでこの手順を繰り返します。

ブランディングの無効化

IM and Presence サービスクラスタのブランディングを無効にするには、次の手順を使用します。

（注） ブランディングを無効にするには、特権レベル 4 のアクセス権を持つマスター管理者アカウントを使用する必要があります。これは、インストール時に作成されるメインの管理者アカウントです。

（注） GUI と CLI のいずれか 1 つだけを使用して、ブランド化を有効にし、無効にするようにしてください。たとえば、GUI インターフェースを使用してブランド化を有効にする場合、GUI インターフェース自体を使用してブランド化を無効にする必要があります。そうしないと、正しく機能しません。

手順

Step 1 Cisco Unified IM and Presence OS の管理にログインします。

Step 2 **[ソフトウェアアップグレード（Software Upgrades）] > [ブランディング（Branding）]** を選択します。

Step 3 [ブランディングの無効化（Disable Branding）] をクリックします。

（注） また、**utils branding disable** CLI コマンドを実行して、ブランディングを無効にすることもできます。

Step 4 変更内容を表示するには、ブラウザを更新します。

Step 5 すべての IM and Presence サービスのクラスタ ノードでこの手順を繰り返します。

ブランディング ファイルの要件

カスタマイズされたブランディングをシステムに適用する前に、仕様に従って `Branding.zip` ファイルを作成します。リモートサーバ上で、ブランディングフォルダを作成し、指定されたコンテンツをフォルダに入れます。すべてのイメージ ファイルとサブフォルダを追加したら、フォルダ全体を圧縮し、ファイルを `branding.zip` として保存します。

ヘッダーに勾配効果を作成するために、ヘッダーに単一のイメージを使用するか、または 6 つのイメージの組み合わせを使用するかに応じて、フォルダー構造に 2 つのオプションがあります。

表 *27:* フォルダ構造オプション

ブランディング オプション	フォルダ構造

単一ヘッダー オプション	ヘッダーの背景（吹き出し項目 3）に 1 つのイメージが必要な場合は、ブランディング フォルダに次のサブフォルダとイメージ ファイルが含まれている必要があります。
	
	`Branding (folder)`
	`  cup (folder)`
	`  BrandingProperties.properties (properties file)`
	`  brandingHeader.gif (652*1 pixel)`
	`  ciscoLogo12pxMargin.gif (44*44 pixel)`

ブランディング オプション	フォルダ構造
グレーディング ヘッダー オプション	ヘッダーの背景（吹き出し項目 3、4、5）に勾配イメージを作成する場合は、勾配効果を作成するために 6 つの個別のイメージ ファイルが必要です。ブランディング フォルダには、これらのサブフォルダとファイルが含まれている必要があります。 Branding(folder) cup (folder) BrandingProperties.properties (file) brandingHeaderBegLTR.gif (652*1 pixel image) brandingHeaderBegRTR.gif (652*1 pixel image) brandingHeaderEndLTR.gif (652*1 pixel image) brandingHeaderEndRTR.gif (652*1 pixel image) brandingHeaderMidLTR.gif (652*1 pixel image) brandingHeaderMidRTR.gif (652*1 pixel image) ciscoLogo12pxMargin.gif (44*44 pixel image)

ユーザ インターフェイスのブランディング オプション

次の画像に、[Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスのブランディング オプションを示します。

図 ***10:*** 管理ログイン画面のブランディング オプション

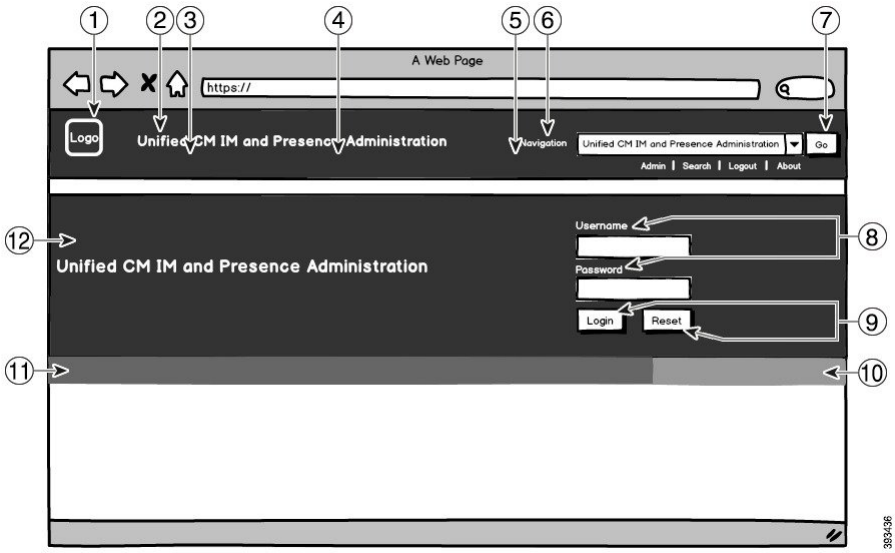
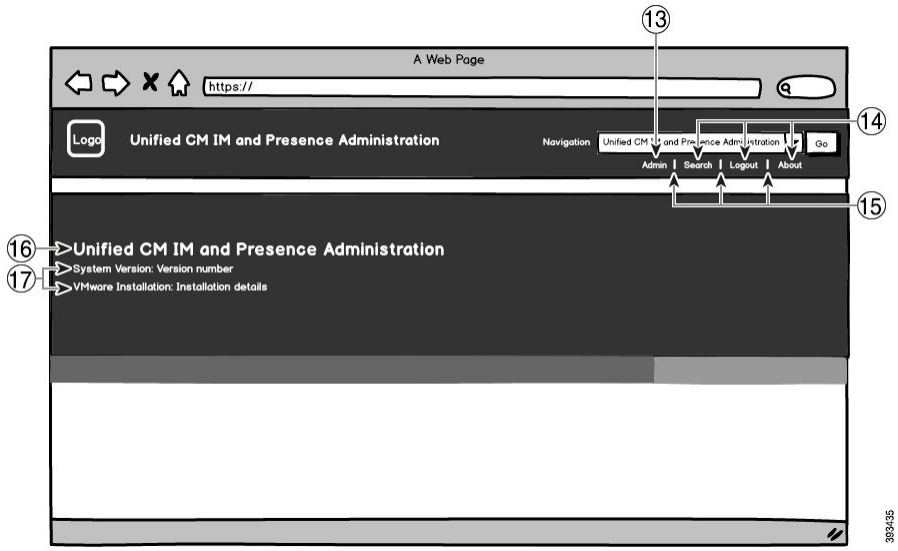


図 *11 :* 管理ログイン中の画面のブランディング オプション



次の表では、上記のスクリーンキャプチャのコールアウト項目をカスタマイズする方法について説明します。

表 *28 :* ユーザ インターフェイスのブランディング オプション

項目	説明	ブランディングの編集
ログイン画面イメージ		
1	企業ロゴ（Company Logo）	IM and Presence サービス インターフェイスにロゴを追加するには、会社のロゴを次のファイル名で 44x44 ピクセル イメージとして保存します。 `ciscoLogo12pxMargin.gif`（44*44 ピクセル）
2	ヘッダーの Unified CM IM and Presence Administration のテキスト	header.heading.color
3	ヘッダーの背景 (採点オプション-左)	ヘッダーイメージに対して採点効果を適用する場合は、左側に次のイメージを使用します。 • `brandingHeaderBegLTR.gif`（652 x 1 ピクセル） • `brandingHeaderBegLTR.gif`（652 x 1 ピクセル）

項目	説明	ブランディングの編集
4	ヘッダーバックグラウンド	ヘッダーに単一のイメージを使用する場合は、次のようにします。 • brandingHeaderMidLTR.gif（652 x 1 ピクセル） それ以外の場合、採点効果があるヘッダーを作成する場合は、次の画像を使用します。 • brandingHeaderMidLTR.gif（652 x 1 ピクセル） • brandingHeaderMidRTR.gif（652 x 1 ピクセル）
5	ヘッダーの背景 (採点オプション-右)	ヘッダーに対して採点効果を使用する場合は、次の画像を右側のヘッダーに使用します。 • brandingHeaderEndLTR（652 x 1 ピクセル） • brandingHeaderEndRTR（652 x 1 ピクセル）
6	ナビゲーション テキスト	header.navigation.color
7	[移動（Go）] ボタン	header.go.font.color header.go.background.color
8	ユーザ名およびパスワードのテキスト	splash.loginfield.color
9	ログインボタンとリセットボタン	splash.button.text.color splash.button.color
10	背景下の色：右側	splash.hex.code.3
11	背景下の色：左側	splash.hex.code.2
12	Banner	splash.hex.code.1
ログイン後イメージ		
13	ログインしているユーザテキスト (たとえば、「admin」ユーザ)	header.text.bold.color
14	検索、情報、ログアウトリンク	header.link.color

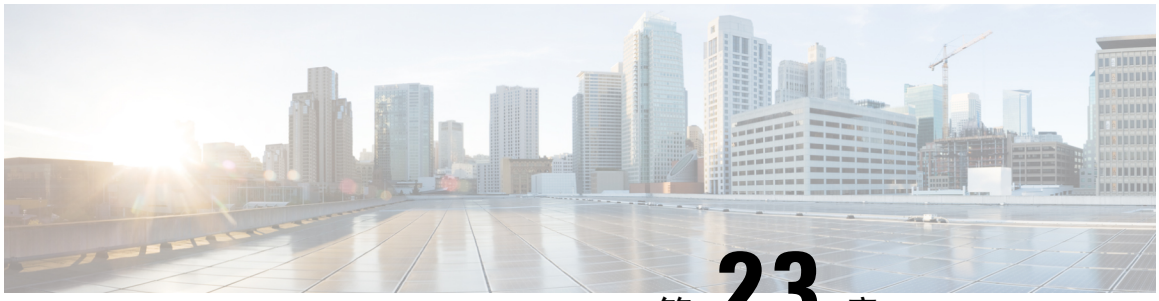
項目	説明	ブランディングの編集
15	リンク区切り線	header.divider.color
16	バナーの Unified CM IM and Presence Administration のテキスト（ログイン後）	splash.login.text.color
17	システムのバージョンおよびVMwareインストールのテキスト	splash.version.color

ブランディング プロパティの編集例

ブランディング プロパティは、プロパティ ファイル（`BrandingProperties.properties`）に16進コードを追加することで編集できます。プロパティ ファイルはHTMLベースの16進コードを使用します。たとえば、ナビゲーションテキスト項目（吹き出し項目#6）の色を赤に変更する場合は、プロパティ ファイルに次のコードを追加します。

```
header.navigation.color="#FF0000"
```

このコードで、`header.navigation.color` は編集するブランディング プロパティで、`"#FF0000"` は新しい設定（赤）です。



第 23 章

拡張機能の設定

ストリーム管理

IM and Presence Service では、インスタントメッセージングのストリーム管理がサポートされています。ストリーム管理は、XEP-0198 仕様を使用して実装されています。これは、2 つの XMPP エンティティ間 (スタンザ受信確認とストリームの再開の機能を含む) をアクティブに管理するための Extensible Messaging and Presence Protocol (XMPP) を定義します。XEP-0198 の詳細については、次の仕様を参照してください。http://xmpp.org/extensions/xep-0198.html

IM and Presence Service と Cisco Jabber 間の通信が一時的に失われた場合、ストリーム管理によって、通信の停止中に送信されるすべてのインスタントメッセージが失われることはありません。設定可能なタイムアウト期間によって、メッセージの処理方法が決まります。

- Cisco Jabber がタイムアウト期間内に IM and Presence Service との通信を再確立した場合、メッセージは再送信されます。
- Cisco Jabber が IM and Presence Service との通信をタイムアウト期間内に再確立しない場合 、メッセージは送信者に返されます。
- タイムアウト期間の経過後に送信されたメッセージはオフラインで保存され、Cisco Jabber が IM and Presence Service との通信を再開するときに配信され ます。

ストリーム管理は、デフォルトでクラスタ全体で有効になっています。ストリーム管理サービスパラメータを使用すると、この機能を設定できます。

ストリーム管理の設定

IM and Presence Service のストリーム管理（XEP-0198）を設定するには、次の手順を使用します。

手順

Step 1 Cisco Unified CM IM and Presence 管理で、**[システム（System）] > [サービスパラメータ（Service Parameters）]** を選択します。

Step 2 **サーバ** ドロップダウンから、IM and Presence ノードを選択します。

Step 3 **サービス** ドロップダウンから、**Cisco XCP ルータ** を選択します。

Step 4 [ストリーム管理の有効化（Enable Stream Management）] サービスパラメータを [有効（Enabled）] に設定します。

Step 5 [ストリーム管理パラメータ（クラスタ全体）（Stream Management Parameters (Clusterwide)）] で、ストリーム管理パラメータを設定します。

表 *29 :* ストリーム管理サービスパラメータ

サービス パラメータ	説明
ストリーム管理の有効化	ストリーム管理のクラスタ全体を有効または無効にします。デフォルトの設定はイネーブルです。
ストリーム管理のタイムアウト	切断されたセッションを再開できる期間の長さ（秒数）は、タイムアウトによって制御されます。クライアントがより長いタイムアウトをネゴシエートしようとした場合（または希望するタイムアウトを指定しなかった場合）、この最大値が適用されます。 このタイムアウト後に送信されたメッセージはすべて、Cisco Jabber が IM and Presence Service を使用して再度ログインする前に、オフラインで保存され、再度ログインした後に再送信 されます。 指定範囲は 30 秒～ 90 秒です。デフォルト値は 60 秒です。
ストリーム管理バッファ（Stream Management Buffer）	ストリーム管理が有効なセッションのバッファに保持される、パケット（パケット履歴）の最大数を定義します。バッファで利用できる履歴よりも多くの履歴をクライアントが必要としている場合、ストリームの再開は失敗します。 指定範囲は 5 ～ 150 パケットで、デフォルト値は 100 パケットです。
確認応答リクエスト率	クライアントに対して最後に受信したスタンザのカウントを提供するように要求する前に、サーバーが送信するスタンザの数を定義します。値を小さくするとネットワークトラフィックが増加しますが、サーバでのスタンザ履歴バッファの削減に役立ち、メモリの使用量が減少します。 この範囲は 1 ～ 64 スタンザで、デフォルト値は 5 です。 （注） 確認応答リクエスト率が小さいと、ネットワークトラフィックが増加しますが、メモリ使用量は減少します。

Step 6 [保存（Save）] をクリックします。

Microsoft Outlook カレンダー統合

Microsoft Outlook の予定表/会議のステータスを IM and Presence Service サーバのプレゼンス ステータスに組み込むことができます。ユーザが会議に出席している場合、そのステータスはユーザのプレゼンス ステータスの一部として表示されます。この機能は、IM and Presence Service をオンプレミス Microsoft Exchange Server またはホスト型 Office 365 サーバに接続することによって実現することができます。

Microsoft Outlook とカレンダーの統合を設定する方法の詳細は、http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html の *IM and Presence Service Microsoft Outlook* 予定表統合ガイドを参照してください。

フェデレーション

IM and Presence Service では、IM and Presence Service が管理する任意のドメイン内からフェデレーション ネットワークを作成することができます。フェデレーション展開には、以下の 2 つの主要なタイプがあります。

- ドメイン間フェデレーション：この統合により、IM and Presence Service が管理する任意のドメイン内のユーザが、外部ドメインユーザとアベイラビリティ情報およびインスタントメッセージング（IM）を交換することができます。外部ドメインは、Microsoft、Google、IBM、または AOL サーバによって管理されている場合があります。IM and Presence Service は、さまざまなプロトコルを使用して、外部ドメイン内のサーバと通信することが可能です。
- パーティション分割された ドメイン内フェデレーション：この統合により、IM and Presence Service と Microsoft サーバ（たとえば、Microsoft Lync）は、共通のドメインまたは一連のドメインをホストします。この統合によって、単一の企業内の IM and Presence Service クライアント ユーザと Microsoft Lync ユーザがインスタント メッセージングおよびアベイラビリティを交換することができるようになります。
- SIP オープンフェデレーション：Cisco IM and Presence サービスは、Cisco Jabber クライアントで SIP オープンフェデレーションをサポートします。管理者は SIP オープンフェデレーションを設定して、Cisco Jabber ユーザが、利用可能なすべてのドメインのユーザとのシームレスなフェデレーションを行えるようにすることができます。オープンフェデレーションは、単一のスタティックルートを使用するすべてのドメインに対して設定できます。スタティックルートにより、Cisco Jabber は任意の外部ドメインとフェデレーションを行うことができます。さらに重要な点として、個々のドメインに対して SIP フェデレーションを設定および管理する場合にかかる時間が大幅に削減されます。

詳細な設定手順は、http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html の *Cisco Unified Communications Manager* での *IM and Presence Service* に対するドメイン間フェデレーション あるいは *Cisco Unified Communications Manager* の *IM and Presence Service* 用のパーティション化ドメイン内フェデレーションを参照してください。

メッセージ アーカイバ

多くの業界では、インスタントメッセージが、他のビジネスレコードと同じ適合認定のガイドラインに従うことが求められています。これらの規制を順守するには、ご使用のシステムがすべてのビジネス レコードを記録してアーカイブする必要があり、アーカイブされたレコードが取得可能になっている必要があります。

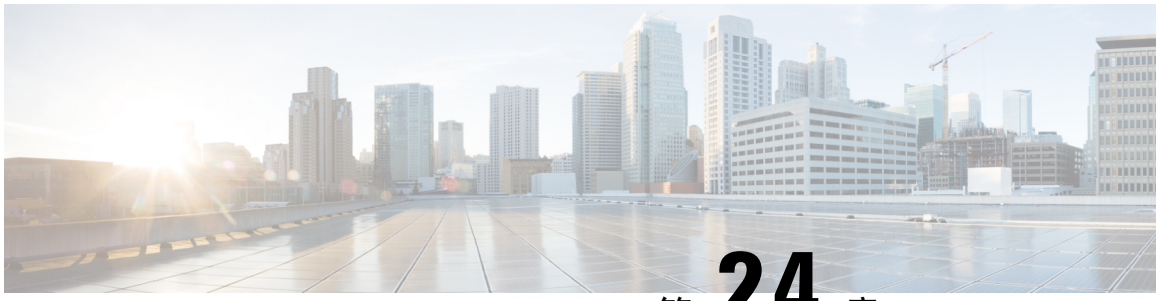
IM and Presence Service は、単一クラスタ ネットワーク構成、クラスタ間ネットワーク構成、または連動ネットワーク構成における以下の IM アクティビティ用のデータを収集して、インスタント メッセージング（IM）コンプライアンスに対するサポートを提供します。

- ポイントツーポイント メッセージ
- グループ チャット： これには、Ad-hoc または一時チャット メッセージと、常設チャット メッセージがあります。
- IM Compliance のコンポーネント
- IM Compliance 用サンプル トポロジおよびメッセージ フロー

IM コンプライアンスの設定の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.htmlの*Cisco Unified Communications Manager* での *IM and Presence Service* のインスタント メッセージ コンプライアンスを参照してください。

第 IV 部

システムの管理



第 24 章

チャットの管理

チャット管理の概要

IM and Presence Service は、チャット ルームを管理し、チャット ルームにアクセスできるユーザを制御するために使用できる設定を提供します。以下の機能が含まれます。

- 新しいルームを作成したり、作成したルームのメンバーおよび設定を管理します。
- メンバーだけがアクセスである常設チャット ルームへのアクセスの制限。
- チャット ルームへの管理者の割り当て。
- ルームへの他のユーザの招待。
- ルームに表示されるメンバーのプレゼンス ステータスの確認。ルームに表示されるプレゼンス ステータスは、ルームへのメンバーの参加を示しますが、全体のプレゼンス ステータスが反映されないことがあります。

IM and Presence Service を使用すると、チャット ノードのエイリアスを管理することもできます。チャット ノード エイリアスを使用すると、ユーザは特定のノード上の特定のチャット ルームを検索して、参加することができます。

さらに、IM and Presence Service はトランスクリプトを保存し、チャット ルームに参加したばかりのメンバーを含むルーム メンバーにこのチャットルームの履歴が利用できるようにします。新規または古くからのメンバーが使用可能な既存のアーカイブのサイズは設定可能です。。

チャット ノード エイリアスの概要

システムの各チャット ノードに一意のエイリアスが必要です。チャット ノード エイリアスは、（任意のドメイン内の）ユーザが特定のノード上の特定のチャット ルームを検索し、これらの

ルームのチャットに入室できるように各チャット ノードに一意のアドレスを作成します。チャット ノードのエイリアスは、そのノード上に作成される各チャット ルームの一意の ID の一部を形成します。たとえば、エイリアス conference-3-mycup.cisco.com は、そのノード上に作成されるチャット ルーム名に使われて、roomjid@conference-3-mycup.cisco.com となります。

チャット ノードのエイリアスを割り当てるには、以下の 2 つのモードを使用します。

- システム生成: 各チャットノードに一意のエイリアスが自動的に割り当てられます。システムは、命名規則 conference-x-clusterid.domain を使用して、デフォルトではチャット ノード毎に 1 個のエイリアスを自動生成します。
  - conference はハードコードされたキーワードです
  - x は、ノード ID を示す一意の整数値です
  - clusterid は設定されたエンタプライズ パラメータです
  - domainが設定されているドメイン

  たとえば、システムは、conference-3-mycup.cisco.comと割り当てられていることができます。
- 手動：チャットノードエイリアスを手動で割り当てることができるようにするには、システム生成エイリアスを無効にしなければなりません。手動管理されたエイリアスでは、特定の要件に合うエイリアスを使用してチャット ノードに名前を付けられるため、完全な柔軟性が提供されます。たとえば、congerence-x-clusterid.domain という命名規則が導入のニーズに合わない場合、このオプションを使用することができます。

ノードあたり複数のエイリアスの割り当て

ノード単位で各チャット ノードに複数のエイリアスを関連付けることができます。ノードごとに複数のエイリアスを関連付けると、ユーザはこれらのエイリアスを使用して追加のチャット ルームを作成できます。この機能は、システム生成のエイリアスおよび手動で作成されたエイリアスの両方に適用されます。

チャット管理の要件

常設のチャットが有効になっていることを確認します。

チャット管理タスク フロー

手順

	コマンドまたはアクション	目的
Step 1	チャットルーム オーナーのチャットルーム設定の編集機能を有効にする（302ページ）	チャット ルームのオーナーがチャットルームの設定を編集できるようにするかどうかを設定します。編集できるようにしない場合は、管理者のみがチャットルームの設定を編集することができます。
Step 2	クライアントでのインスタント メッセージ履歴のログ記録の許可 （303 ページ）	ユーザがコンピュータでインスタントメッセージ履歴をローカルにログ記録することを防止または許可することができます。
Step 3	常設チャットルームの作成をホームクラスタに制限する （303 ページ）	この手順を使用して、Cisco Jabber ユーザのホームクラスタ内での常駐チャットルームの作成を制限します。
Step 4	外部データベース Text Conferencing Report の表示 （304 ページ）	常設チャットルームの詳細を提示する外部データベース Text Conferencing Report を表示するには、以下の手順を使用します。
Step 5	常設チャットルームの所有権の譲渡（305ページ）	この手順を使用して、ホーム クラスタに属する常設チャットルームの所有権を、チャットルームの他の既存のメンバーに転送します。
Step 6	常設チャットエイリアスレポート （306ページ）	この手順を使用して、外部データベースに存在する独自およびピアクラスタエイリアスのチャットルーム数を表示します。
Step 7	チャット ルームの設定を編集します。以下のタスクのいずれかを任意の順序で実行して、チャット ルームの設定を変更します。 • チャット ルーム数の設定 （307 ページ） • チャット ルームのメンバー設定の構成 （307 ページ） • 可用性の設定 （309 ページ） • 利用者数の設定 （310 ページ）	（注） 常設チャットの設定を更新する場合は、Cisco Unified IM and Presence Serviceability 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）]** を選択して、Cisco XCP Text Conference Manager サービスを再起動します。

	コマンドまたはアクション	目的
	• チャットメッセージの設定（311 ページ） • モデレータが管理するルームの設定（312 ページ） • 履歴の設定 （313 ページ）	
Step 8	チャットルームのシステムデフォルト設定へのリセット （313 ページ）	チャットの設定をシステムのデフォルトにリセットする場合は、以下のオプション タスクを実行します。アドホック チャットはデフォルトで有効に、常設チャットはデフォルトでは無効に設定されています。このタスクを完了すると、常設チャットは無効となります。
Step 9	チャット ノードのエイリアスの管理（314 ページ）	エイリアスは、（任意のドメイン内の）ユーザが特定のノード上の特定のチャット ルームを検索し、これらのルームのチャットに入室できるように各チャット ノードに一意のアドレスを作成します。システムの各チャット ノードに一意のエイリアスが必要です。
Step 10	常設チャット用の外部データベースのクリーンアップ （317 ページ）	オプション。外部データベースのクリーンアップ ユーティリティを使用して、外部データベースを監視するジョブを設定し、期限切れのレコードは削除します。これで、常に最新のレコードのために十分なディスク スペースが確保されます。

チャット ルーム オーナーのチャット ルーム設定の編集機能を有効にする

チャットルームのオーナーがチャットルームの設定を編集できるようにする場合は、この手順を使用します。

（注） クライアントからこれらの設定をどの程度行えるかは、クライアントの実装や、クライアントがこれらの設定を行うインターフェイスを提供しているかどうかで決まります。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**メッセージング** > **グループ チャット および 常設チャット**を選択します。

Step 2 **ルームのオーナーはルームをメンバー専用にするかどうかを変更できる**チェック ボックスの値を設定します。

- オン：チャットルームのオーナーは、チャットルームの設定を編集する管理機能を利用することができます。
- オフ：管理者のみがチャット ルームの設定を編集することができます。

Step 3 **[保存（Save）]** をクリックします。

Step 4 **Cisco Unified IM and Presence Serviceability**で、**ツール** > **コントロール センター - 機能サービス**を選択します。

Step 5 Cisco XCP Text Conference Manager サービスを再起動します。

クライアントでのインスタント メッセージ履歴のログ記録の許可

ユーザがコンピュータでインスタント メッセージ履歴をローカルにログ記録することを防止または許可できます。クライアント側では、アプリケーションがこの機能をサポートしている必要があります。これは、インスタント メッセージのログ記録の防止を実行する必要があります。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**メッセージング** > **設定**を選択します。

Step 2 次のようにインスタント メッセージ履歴のログ記録の設定を行います。

- クライアント アプリケーションのユーザに IM and Presence Service でインスタント メッセージのログ記録を許可するには、**クライアントでのインスタントメッセージ履歴のログ記録を可能にする(サポートされているクライアントのみ)**をオンにします。
- クライアント アプリケーションのユーザに IM and Presence Service でインスタント メッセージ履歴のログ記録を許可しない場合は、**クライアントでのインスタントメッセージ履歴のログ記録を可能にする(サポートされているクライアントのみ)**をオフにします。

Step 3 [保存（Save）] をクリックします。

常設チャットルームの作成をホームクラスタに制限する

Important この機能は、リリース 14 SU1 以降で適用されます。

この手順を使用して、Cisco Jabber ユーザのホームクラスタ内での常駐チャットルームの作成を制限します。この機能により、クラスタ間のトラフィックが減少し、システム帯域幅が増加します。

IM and Presence サービス管理者は、ホームクラスタでユーザによって作成されたすべてのチャットルームを管理します。他のクラスタのメンテナンスアクティビティは、ホームクラスタ内のユーザによって作成されたチャットルームには影響しません。

Before you begin

Important リリース 14SU1 以降でサポートされます。

- 常設チャットが有効になっていることを確認します。
- この機能を有効にする前に、**グループチャットと常設チャットの設定**ウィンドウの**エイリアスレポート**を確認してください。詳細については、常設チャットエイリアスレポート, on page 306を参照してください。
- この機能をサポートするには、Cisco Jabber 14.1 バージョン以降が必要です。

Procedure

Step 1 データベース パブリッシャ ノードで **Cisco Unified CM IM and Presence 管理**にログインします。

Step 2 **[メッセージング]** > **[グループチャットと永続的なチャット]** を選択します。

Step 3 **[常設チャットを有効にする（Enable Persistent Chat）]** で、**[ルームの作成をホーム クラスタに制限する（Limit room creation to home cluster）]** チェックボックスをオンにします。

What to do next

ホームクラスタ内のすべてのノードで **Cisco XCP Text Conference Manager サービス**を再起動します。

外部データベース Text Conferencing Report の表示

外部データベースの Text Conferencing Report を表示するには、次の手順を使用します。このレポートでは、導入環境内の常設チャットルームとアドホックチャットルームの詳細が表示されます。

手順

Step 1 **Cisco Unified CM IM and Presence Administration** にログインします。

Step 2 **[メッセージング]** > **[グループチャットと永続的なチャット]** を選択します。

Step 3 **[常設チャットデータベースの割り当て（Persistent Chat Database Assignment）]** の下の **[ルームレポート（Room Report）]** ボタンをクリックします。

Step 4 特定の条件を満たすルームだけを選択するには、フィルタ ツールを使用します。

Step 5 [検索（Find）] をクリックします。

Step 6 特定のチャットルームを選択すると、そのルームの詳細が表示されます。

（注） データベースから取得されるレコードの数は、[取得されたレコード] ドロップダウンリストから選択した値によって異なります。

常設チャットルームの所有権の譲渡

重要 この機能は、リリース 14 SU1 以降で適用されます。

GUI にアクセスできる IM and Presence Service 管理者が常設チャットルームの所有権を転送するには、この手順を使用します。

たとえば、John は常設チャットルームを作成し、数人のメンバーを追加しましたが、後で組織を去ったとします。

John が唯一の常設チャットルームの所有者であり、特定のルームにルームのオーナーの機能が引き続き必要な場合、IM and Presence サービスの管理者は、1 人以上の現在のルームメンバーを新しいルームのオーナーとして選択できます。

オーナー ID を更新するときは、次の点を考慮してください。

- チャットルームの所有権を、前の所有者と同じホームクラスタに属するチャットルームメンバーに変更できます。
- **オーナー ID** は、**ユーザ ID** ではなく、**ユーザ JID** である必要があります。
- 入力された**オーナー ID** は、IM and Presence サービスノードデータベースに対して検証されます。
- 管理者は、チャットルームの新しいオーナー ID としてルーム作成者の ID を設定できません。

チャットルームの所有権を変更するには、次の手順を実行します。

始める前に

重要 リリース 14SU1 以降でサポートされます。

オーナー ID を更新する前に、ホームクラスタ内のすべての IM and Presence サービスノードで **Cisco XCP Text Conference Manager サービス**を停止します。

手順

Step 1 データベース パブリッシャ ノードで **Cisco Unified Communications Manager IM and Presence Service Administration** にログインします。

Step 2 **[メッセージング（Messaging）]** > **[グループチャットとパーシステントチャット（Group Chat and Persistent Chat）]** と選択します。

Step 3 **[常設チャットデータベースの割り当て（Persistent Chat Database Assignment）]** の下の **[ルームレポート（Room Report）]** ボタンをクリックします。

Step 4 特定の条件を満たすルームだけを選択するには、フィルタツールを使用して、**[検索（Find）]** をクリックします。

Step 5 （オプション）**[ルーム JID（Room JID）]** をクリックして、所有者のリスト、メンバーのリスト、最後のメッセージの日付などの PChat ルームのフィールドを表示します。フィールドの詳細や説明については、オンラインヘルプを参照してください。

Step 6 **[ルーム JID（Room JID）]** のチェックボックスをオンにして、**[オーナー ID（Owner ID）]** フィールドを編集します。

（注） **[オーナー ID（Owner ID）]** 列は、ホームクラスタに属する常設チャットルームに対してのみ編集できます。

Step 7 新しいオーナーにするチャットルームメンバーの**オーナー ID** をメール形式で入力します。

Step 8 **[オーナー ID の更新（Update Owner ID）]** をクリックします。
これにより、選択した 1 つ以上の常設チャットルームの所有者が同じ**オーナー ID** で更新されます。

次のタスク

ホームクラスタ内のすべてのノードで **Cisco XCP Text Conference Manager サービス**を開始します。

常設チャットエイリアスレポート

この手順を使用して、外部データベースの常設チャットエイリアスレポートを表示します。このレポートでは、チャットルームの数と、外部データベースに存在するホームクラスタエイリアスとピアクラスタエイリアスを表示できます。

Procedure

Step 1 データベース パブリッシャ ノードで **Cisco Unified CM IM and Presence 管理**にログインします。

Step 2 **[メッセージング]** > **[グループチャットと永続的なチャット]** を選択します。

Step 3 **[常設チャット データベースの割り当て（Persistent Chat Database Assignment）]** で、ドロップダウン リストから **[外部データベース（External Database）]** を選択します。

Step 4 **[エイリアスレポート（Alias Report）]** ボタンをクリックします。フィールドの説明については、オンライン ヘルプを参照してください。

チャット ルームの設定

チャット ルーム数の設定

ユーザが作成できるルーム数を制限するには、ルーム設定を使用します。チャット ルームの数を制限すると、システムのパフォーマンスがサポートされ、拡張性が許容されます。ルーム数の制限は、起こり得るサービス レベル攻撃の軽減にも役立ちます。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**メッセージング** > **グループ チャット および 常設チャット**を選択します。

Step 2 許可したチャット ルームの最大数を変更するには、[許可されるルームの最大数（Maximum number of rooms allowed）] のフィールドに値を入力します。デフォルトでは 5500 に設定されています。

Step 3 [保存（Save）] をクリックします。

チャット ルームのメンバー設定の構成

メンバー設定で、チャット ルームのメンバーシップをシステム レベルで制御することができます。こういった制御は、禁止などの管理操作によって防止できるサービス レベル攻撃を軽減する上で役立ちます。必要に応じてメンバーを設定します。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**メッセージング** > **グループ チャット および 常設チャット**を選択します。

Step 2 ルーム メンバーの設定の説明に従って、ルーム メンバー設定を構成します。

Step 3 **[保存（Save）]** をクリックします。

Step 4 **Cisco Unified IM and Presence Serviceability**で、**ツール** > **コントロール センター - 機能サービス**を選択します。

Step 5 Cisco XCP Text Conference Manager サービスを再起動します。

ルーム メンバーの設定

（注） 常設チャットルームは、作成時の設定を継承します。後で行った変更は、既存のルームには適用されません。これらの変更は、変更が有効になった後に作成されたルームにのみ適用されます。

表 30 :

フィールド	説明
デフォルトではルームはメンバー専用です（Rooms are for members only by default）	ルームを作成する際にメンバー専用をデフォルト設定にする場合には、このチェックボックスをオンにします。メンバー専用ルームには、そのルームのオーナーまたは管理者が設定した許可リストのユーザのみがアクセスすることができます。このチェックボックスは、デフォルトでオフになっています。 （注） 許可リストにはそのルームに許可されているメンバーのリストが含まれています。このリストは、メンバー専用ルームの所有者または管理者によって作成されます。
他のユーザをメンバー専用ルームに招待できるのはモデレータのみです（Only moderators can invite people to members-only rooms）	モデレータのみがルームへのユーザの招待を行うことができるようにルームを設定する場合は、このチェックボックスをオンにします。このチェックボックスをオフにしている場合は、メンバーが他のユーザをルームに参加するよう招待できます。デフォルトでは、このチェックボックスはオフになっています。
ルームのオーナーは、ルームをメンバー専用にするかどうかを変更できます（Room owners can change whether or not rooms are for members only）	ルームをメンバー専用にするかどうかをルーム オーナーが変更できるように設定する場合は、このチェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。 （注） ルーム所有者は、そのルームを作成したユーザか、（許可されている場合は）ルーム作成者または所有者によって所有者ステータスを持つ者として指定されたユーザです。ルーム所有者は、ルーム設定の変更やルーム破棄のほか、その他のすべての管理機能を実行できます。

フィールド	説明
ルームのオーナーは、他のユーザをメンバー専用ルームに招待できるのはモデレータに限定するかどうかを変更できます（Room owners can change whether or not only moderators can invite people to members-only rooms）	ルームの所有者にメンバーが他のユーザをルームに招待できるようにルームを設定するには、このチェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。
ユーザは自分自身をメンバーとしてルームに追加できます（Users can add themselves to rooms as members）	すべてのユーザが随時ルームへの参加要求ができるように設定する場合は、このチェックボックスをオンにします。このチェックボックスがオンになっている場合、ルームはオープン メンバーシップになります。デフォルトで、このチェックボックスはオフになっています。
ルームのオーナーは、ユーザが自分自身をメンバーとしてルームに追加できるようにするかどうかを変更できます（Room owners can change whether users can add themselves to rooms as members）	ステップ 5 に記載された設定をルーム オーナーが随時変更可能であるようにルームを設定する場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。

可用性の設定

可用性の設定は、ルーム内のユーザの可視性を決定します。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**メッセージング** > **グループ チャット および 常設チャット**を選択します。

Step 2 アベイラビリティ設定の箇所で説明されるように、アベイラビリティのメンバー設定を構成します。

Step 3 **[保存（Save）]** をクリックします。

Step 4 **Cisco Unified IM and Presence Serviceablity**で、**ツール** > **コントロール センター - 機能サービス**を選択します。

Step 5 Cisco XCP Text Conference Manager サービスを再起動します。

アベイラビリティの設定

フィールド	説明
ルーム内にいないメンバーや管理者がルームに表示されたままです（Members and administrators who are not in a room are still visible in the room）	その時にオフラインのユーザでもルームの名簿に記載したままにするには、このチェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。 （注） 管理者がチャットルームを離れても、管理者のユーザ ID はチャットルームに表示されます。ユーザのリストを更新するには、チャットルームを閉じてから再度開く必要があります。
ルームのオーナーは、ルーム内にいないメンバーや管理者がルームに表示されたままにするかどうかを変更できます（Room owners can change whether members and administrators who are not in a room are still visible in the room）	ルームのオーナーがメンバーまたは管理者の表示を変更できるようにするには、このチェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。
ルームは古いクライアントと下位互換性があります（Rooms are backwards-compatible with older clients）	以前の グループ チャット 1.0 クライアントを使用したサービスを適切に機能させる場合は、このチェック ボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。
ルームのオーナーは、ルームが古いクライアントと下位互換性があるかようにするどうかを変更できます（Room owners can change whether rooms are backwards-compatible with older clients）	ルーム オーナーがチャット ルームの下位互換性を制御できるようにするには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。
デフォルトで、ルームは匿名です（Rooms are anonymous by default）	ルームにユーザのニックネームは表示しても、Jabber ID は公開しない場合は、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。
ルームのオーナーは、ルームを匿名にするかどうかを変更できます（Room owners can change whether or not rooms are anonymous）	ユーザの Jabber ID の匿名レベルをルーム オーナーが管理できるようにする場合は、このチェック ボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。

利用者数の設定

利用者数の設定では、特定の時間にチャット ルームに参加することができるユーザ数を指定します。

手順

Step 1 ルーム内で許可されるユーザのシステム最大数を変更するには、**[同時にルームに入室できるユーザ数（How many users can be in a room at one time）]** のフィールドに値を入力します。デフォルト値は 1000 に設定されています。

（注） ルーム内のユーザの総数は、設定する値を超えることはできません。ルーム内のユーザの総数には、通常のユーザと非表示のユーザの両方が含まれます。

Step 2 ルーム内で許可される非表示ユーザの数を変更するには、**[同時に入室できる非表示ユーザ数（How many hidden users can be in a room at one time）]** のフィールドに値を入力します。非表示のユーザは他のユーザには表示されません。また、ルームにメッセージを送信できません。さらに、プレゼンス更新を送信しません。非表示のユーザは、ルーム内のすべてのメッセージを表示したり、他のユーザのプレゼンス更新を受信したりできます。デフォルト値は 1000 です。

Step 3 ルーム内に許可されるユーザのデフォルトの最大数を変更するには、**[デフォルトのルーム最大利用者数（Default maximum occupancy for a room）]** のフィールドに値を入力します。デフォルト値は 50 に設定され、ステップ 1 で設定された値よりも大きくできません。

Step 4 デフォルトのルーム利用者数をルーム所有者が変更できるようにする場合は、**[ルーム所有者がデフォルトのルーム最大利用者数を変更できます（Room owners can change default maximum occupancy for a room）]** チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。

Step 5 [保存（Save）] をクリックします。

チャット メッセージの設定

チャット メッセージ設定を使用して、役割に基づいた特権をユーザに付与します。ほとんどの場合、役割は、ビジターからモデレータへの階層に存在します。たとえば、参加者はビジターができることはすべて実行できます。また、モデレータは参加者ができることはすべて実行できます。

デフォルトでは、このチェックボックスはオフになっています。

手順

Step 1 **[Lowest participation level a user can have to send a private message from within the room（ルーム内からプライベート メッセージを送信するためにユーザに必要な最小参加レベル）]** のドロップダウン リストから次のいずれかを選択します。

- **ゲスト**では、ゲスト、参加者、モデレータがルーム内の他のユーザにプライベート メッセージを送信することができます。
- **[参加者（Participant）]** を選択すると、参加者およびモデレータがルーム内の他のユーザにプライベート メッセージを送信できます。
- **[モデレータ（Moderator）]** を選択すると、モデレータのみがルーム内の他のユーザにプライベート メッセージを送信できます。

Step 2 プライベートメッセージの最小参加レベルをルーム所有者が変更できるようにする場合は、**[ルーム内からプライベート メッセージを送信するためにユーザに必要な最小参加レベルをルーム所有者が変更できます（Room owners can change the lowest participation level a user can have to send a private message from within the room）]** チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。

Step 3 [Lowest participation level a user can have to change a room's subject（ルームの件名を変更するためにユーザに必要な最小参加レベル）] のドロップダウン リストから次のいずれかを選択します。

a) **[参加者（Participant）]** を選択すると、参加者およびモデレータがルームの件名を変更できます。これがデフォルトの設定です。

b) **[モデレータ（Moderator）]** を選択すると、モデレータのみがルームの件名を変更できます。

ビジターは、ルームの件名を変更できません。

Step 4 ルームの件名を更新するための最小参加者レベルをルーム所有者が変更できるようにする場合は、**[ルームの件名を変更するためにユーザに必要な最小参加レベルをルーム所有者が変更できます（Room owners can change the lowest participation level a user can have to change a room's subject）]** チェックボックスをオンにします。

Step 5 メッセージからすべての拡張可能ハイパーテキスト マークアップ言語（XHTML）を削除する場合は、**[すべての XHTML フォーマットをメッセージから削除します（Remove all XHTML formatting from messages）]** チェックボックスをオンにします。デフォルトで、このチェックボックスはオフになっています。

Step 6 XHTML フォーマット設定をルーム所有者が変更できるようにする場合は、**[ルーム所有者が XHTML フォーマット設定を変更できます（Room owners can change XHTML formatting setting）]** チェックボックスをオンにします。デフォルトで、このチェックボックスはオフになっています。

Step 7 [保存（Save）] をクリックします。

モデレータが管理するルームの設定

モデレータが管理するルームは、ルーム内のボイス特権を付与または取り消しする機能をモデレータに提供します（グループチャットの場合、ボイスはチャットメッセージをルームに送信する機能のことです）。ビジターはモデレータが管理するルームでインスタント メッセージを送信できません。

手順

Step 1 モデレータの役割をルームで適用する場合は、**[デフォルトでモデレータがルームを管理します（Rooms are moderated by default）]** チェックボックスをオンにします。デフォルトで、このチェックボックスはオフになっています。

Step 2 ルームをモデレータが管理するかどうかをルーム所有者が変更できるようにするには、**[デフォルトでモデレータがルームを管理するかどうかをルーム所有者が変更できます（Room owners can change whether rooms are moderated by default）]** チェックボックスをオンにします。デフォルトでは、このチェックボックスはオフになっています。

Step 3 [保存（Save）] をクリックします。

履歴の設定

履歴設定を使用して、ルームで取得し、表示するメッセージのデフォルト値および最大値を設定し、履歴クエリを使用して取得できるメッセージ数を管理します。ユーザがルームに入室すると、そのユーザはルームのメッセージ履歴に送信されます。履歴設定は、ユーザが受信する過去のメッセージ数を決定します。

手順

Step 1 ユーザがアーカイブから取得できるメッセージの最大数を変更するには、**[アーカイブから取得できるメッセージの最大数（Maximum number of messages that can be retrieved from the archive）]** のフィールドに値を入力します。デフォルト値は 100 に設定されています。これは、次の設定の上限としての役割を果たします。

Step 2 ユーザがチャットルームに入室するときに表示される以前のメッセージの数を変更するには、**[デフォルトで表示されるチャット履歴内のメッセージ数（Number of messages in chat history displayed by default）]** のフィールドに値を入力します。デフォルト値は 15 に設定され、ステップ 1 で設定された値よりも大きくできません。

Step 3 ユーザがチャット ルームに入室したときに表示される以前のメッセージの数をルーム所有者が変更できるようにする場合は、**[ルーム所有者がチャット履歴に表示されるメッセージ数を変更できます（Room owners can change the number of messages displayed in chat history）]** チェックボックスをオンにします。デフォルトで、このチェックボックスはオフになっています。

Step 4 [保存（Save）] をクリックします。

チャット ルームのシステム デフォルト設定へのリセット

グループ チャットの設定をアドホック チャット ルームと常設チャット ルームのシステム デフォルト設定にリセットする場合は、この手順を使用します。

（注） アドホック チャットはデフォルトで有効になっており、常設チャットはデフォルトでは無効となっています。このタスクを完了すると、常設チャットが無効になります

手順

Step 1 **Cisco Unified CM IM and Presence Administration**で、**メッセージング** > **設定**を選択します。

Step 2 [デフォルトに設定（Set to Default）] をクリックします。

Step 3 [保存（Save）] をクリックします。

チャット ノード エイリアスの管理

チャット ノードのエイリアスの管理

クラスタのチャット ノードのエイリアスを管理するには、このタスクを完了してください。システムによる、エイリアスの自動管理あるいは手動更新を設定することができます。

手順

	コマンドまたはアクション	目的
Step 1	チャット エイリアス管理の割り当てモード （314 ページ）	システムでチャット ノードのエイリアスを管理するか、または手動で実行するかを指定します。
Step 2	チャット ノード エイリアスの手動の追加（315 ページ）	クラスタのチャットノ ードのエイリアスを追加、編集、または削除します。

チャット エイリアス管理の割り当てモード

システムがチャット ノード エイリアスを自動で割り当てする設定にする場合は、`conference-x-clusterid.domain naming convention` 命名規則を使用して、チャット ノード エイリアスを自動的に割り当てるか、あるいは手動で割り当てるかを設定します。

始める前に

チャット ノードのエイリアスの詳細については、チャット ノード エイリアスの概要 （299 ページ） を参照してください。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**メッセージング** > **グループ チャット および 常設チャット**を選択します。

Step 2 システムで生成されたエイリアスを有効または無効にします。

- システムが チャット ノード エイリアスを自動的に割り当てる設定にする場合は、**プライマリ グループ チャット サーバのエイリアスをシステムで自動的に管理する**をオンにします。

  ヒント **[Messaging（メッセージング）]** > **[Group Chat Server Alias Mapping（グループ チャット サーバのエイリアス マッピング）]** を選択して、システムで生成されたエイリアスが [Primary Group Chat Server Aliases（プライマリ グループ サーバのエイリアス）] の下にリストされていることを確認します。

- チャットノードエイリアスを手動で割り当てる場合は、**プライマリグループチャットサーバのエイリアスをシステムで自動的に管理する** をオフにします。

次のタスク

- チャット ノードにシステムで生成されたエイリアスを設定する場合でも、ノードと複数のエイリアスを必要に応じて関連付けることができます。
- 外部ドメインとフェデレーションすると、エイリアスが変更され、新しいエイリアスが使用可能であることをフェデレーション相手に通知する場合があります。すべてのエイリアスを外部にアドバタイズするには、DNS を設定し、DNS レコードとしてエイリアスをパブリッシュします。
- システム生成エイリアス設定を更新した場合、これらの操作のいずれかを実行して、Cisco XCP Text Conference Manager を再起動します。
- チャット ノードのエイリアスを追加、編集、または削除するには、チャット ノード エイリアスの手動の追加（315 ページ）。

チャット ノード エイリアスの手動の追加

手動でチャット ノードのエイリアスを追加、編集、または削除する設定にするには、この手順を使用します。手動でチャット ノードのエイリアスを管理するには、システムで生成されたエイリアスを使用するデフォルト設定をオフにする必要があります。システムで生成されたエイリアスをオフにすると、既存のエイリアス（`conference-x-clusterid.domain`）は、[会議サーバのエイリアス（Conference Server Aliases）] の下にリストされる標準の編集可能なエイリアスに戻ります。これで、古いエイリアスとそのエイリアスに関連付けられているチャット ルームのアドレスは維持されます。

チャット ノードに手動で複数のエイリアスを割り当てることができます。システムで生成されたエイリアスがチャット ノードにすでに存在する場合でも、ノードに追加エイリアスを手動で関連付けることができます。

手動管理されるエイリアスでは、クラスタ ID またはドメインが変更された場合、手動でエイリアス リストを更新するのは管理者の責任です。システムで生成されたエイリアスが変更された値を自動的に組み込みます。

（注） これは必須ではありませんが、ノードに新しいチャット ノードのエイリアスを割り当てる場合はドメインを常に含めることを推奨します。追加エイリアスには、newalias.domain の表記を使用します。ドメインを確認するには、**Cisco Unified CM IM and Presence 管理** > **プレゼンス設定** > **詳細設定** を選択します。

始める前に

チャット エイリアス管理の割り当てモード （314 ページ）

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**メッセージング** > **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。

Step 2 [検索（Find）] をクリックします。

グループ チャット サーバの [エイリアス] ウィンドウに、既存のノード エイリアスが表示されます。

Step 3 新しいエイリアスを追加する：

a) [新規追加（Add New）] をクリックします。
b) **グループ チャット サーバ エイリアス** フィールドに新しいエイリアスを入力します。
c) **サーバ名** ドロップダウン リスト ボックスで、エイリアスを割り当てるサーバを選択します。
d) **[保存（Save）]** をクリックします。

Step 4 既存のエイリアスを編集する：

a) エイリアスを選択します。
b) 更新情報を入力し、**保存** をクリックします。

Step 5 エイリアスを削除するには、エイリアスを選択して、**選択項目の削除** をクリックします。

次のタスク

- Cisco XCP Text Conference Manager をオンにします。

チャット ノード エイリアスのトラブル シューティングのヒント

- どのチャット ノードのエイリアスも一意でなければなりません。システムはクラスタ全体に重複したチャット ノードのエイリアスを作成することを防ぎます。
- チャット ノードのエイリアス名を IM and Presence ドメイン名と同じにすることはできません。
- 古いエイリアスでチャット ルームのアドレスを維持する必要がなくなった場合に限り古いエイリアスを削除します。
- 外部ドメインとフェデレーションすると、エイリアスが変更され、新しいエイリアスが使用可能であることをフェデレーション相手に通知する場合があります。すべてのエイリアスを外部にアドバタイズするには、DNS を設定し、DNS レコードとしてエイリアスをパブリッシュします。
- チャット ノードのエイリアス設定のいずれかを更新したら、Cisco XCP Text Conference Manager を再起動します。

常設チャット用の外部データベースのクリーンアップ

外部データベースを監視し、期限切れのレコードを削除するジョブを設定します。これで、常に最新のレコードのために十分なディスク スペースが確保されます。

常設チャット用のデータベース テーブルをクリンナップするには、必ず**機能テーブル**の下の**Text Conference**（**TC**） 機能を選択します。

手順

Step 1 データベース パブリッシャ ノードで Cisco Unified CM IM and Presence Administration にログインします。

Step 2 **メッセージング** > **外部データベースの設定** > **外部データベース** を選択します。

Step 3 **外部 DB のクリア**をクリックします。

Step 4 次のいずれかを実行します。

- パブリッシャ ノードに接続する外部データベースを手動でクリーンアップするには、**samecup ノード**を選択します。
- サブスクライバ ノードに接続する外部データベースを手動でクリーンアップする場合は、**その他の CupNode** を選択してから、外部データベースの詳細を選択します。
- 外部データベースを自動的にモニタおよびクリーンアップするシステム設定の場合は、**自動クリーンアップ** オプション ボタンをオンにします。

（注） 自動クリーンアップを設定する前に、手動でのクリーンアップを実行することを推奨します。

Step 5 いつまでさかのぼってファイル削除をするかの**日数**を設定します。たとえば、90 を入力した場合、システムは 90 日前以前の古いレコードを削除します。

Step 6 データベースのインデックスとストアドプロシージャを作成するには、**スキーマの更新** をクリックします。

（注） スキーマの更新は、このジョブを最初に実行するときにのみです。

Step 7 いつまでさかのぼってファイル削除をするかの**日数**を設定します。たとえば、**90** を入力した場合、システムは 90 日より前の古いレコードを削除します。

Step 8 **機能テーブル** セクションで、レコードをクリーンアップする各機能を選択します。

- **テキスト会議**：常設チャット機能のデータベース テーブルを消去するには、このオプションを選択します。
- **メッセージアーカイバ**（**MA**）: メッセージアーカイバ機能のデータベース テーブルをクリーンアップするには、このオプションを選択します。
- **マネージドファイル転送**（**MFT**）：マネージドファイル転送機能のデータベーステーブルを消去するには、このオプションを選択します。

Step 9 **[クリーンアップジョブを送信**（**Submit Clean-up Job**）**]** をクリックします。

（注） **[自動（Automatic）]** オプションが有効になっていて、それを無効にする場合は、**[自動クリーンアップジョブの無効化（Disable Automatic Clean-up Job）]** ボタンをクリックします。

チャット インタラクションの管理

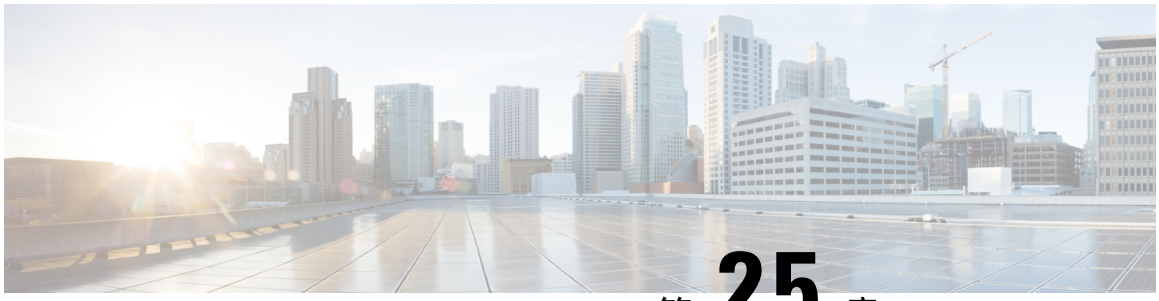
チャットノードのエイリアスを変更すると、データベースのチャットルームのアドレス指定が不可能になり、ユーザが既存のチャット ルームを検索できなくなることがあります。

エイリアスまたは他のノードの依存関係の構成部分を変更する前にこれらの結果に注意してください。

- クラスタ ID：この値は完全修飾クラスタ名（FQDN）の一部です。クラスタ ID を変更（[システム]>[プレゼンス トポロジの設定] を選択）すると、FQDN はクラスタ全体で自動的に変更される新しい値およびシステム管理されたエイリアスを組み込みます。手動管理されたエイリアスでは、クラスタ ID が変更された場合、手動でエイリアス リストを更新するのは管理者の責任です。
- ドメイン：この値はFQDNの一部です。ドメインを変更（[プレゼンス]>[プレゼンスの設定] を選択）すると、FQDN はクラスタ全体で自動的に変更される新しい値およびシステム管理されたエイリアスを組み込みます。手動管理されたエイリアスでは、ドメインが変更された場合、手動でエイリアス リストを更新するのは管理者の責任です。
- チャット ノードと外部データベース間の接続：永続的なチャットが有効で、外部データベースとの適切な接続が維持されていない場合、チャット ノードは起動しません。
- チャット ノードの削除：プレゼンス トポロジから既存のエイリアスに関連付けられているノードを削除した場合、それ以上の処理を行わない限り、その古いエイリアスを使用して作成したチャット ルームをアドレス指定できないことがあります。

変更の広い影響を考慮せずに既存のエイリアスを変更しないことを推奨します。つまり、次のようにします。

- ユーザが必要に応じて古いエイリアスによって既存のチャット ルームを検索することができるように、データベースに古いチャット ノードのアドレスを維持します。
- 外部ドメインとのフェデレーションがある場合、DNS エイリアスをパブリッシュし、エイリアスが変更され、新しいアドレスが使用可能であることをそのドメインのユーザに通知する必要があります。これはすべてのエイリアスを外部にアドバタイズするかどうかによって異なります。



第 25 章

マネージド ファイル転送の管理

マネージド ファイル転送の管理の概要

IM and Presence Service の管理者は、マネージド ファイル転送機能のファイルの保管およびディスク利用の管理を担当します。この章では、ファイル ストレージおよびディスク使用量のレベルを監視し、レベルが指定されたしきい値を超えた際に通知するためのカウンタと警告を設定します。

外部ファイル サーバおよびデータベース サーバの管理

外部データベースのサイズを管理する際は、指定に応じて、ファイルをデータベースから自動的にパージするように、クエリをシェルスクリプトと組み合わせることが可能です。クエリを作成するには、ファイル転送メタデータを使用します。これには、転送タイプ、ファイル タイプ、タイムスタンプ、ファイルサーバ上のファイルへの絶対パス、およびその他の情報が含まれます。

1 対 1 の IM やグループ チャットは通常、一時的なものであり、転送されたファイルはすぐに削除される可能性があります。IM やグループ チャットの処理方法を選択する際には、これを考慮に入れてください。ただし、次の点に注意してください。

- オフライン ユーザに配信される IM のために、ファイルに対する遅延要求が発生する可能性があります。
- 永続的なチャットの転送は、長期間保持される必要がある可能性があります。

（注）

- 現在の UTC 時間中に作成されたファイルは消去しないでください。
- ファイル サーバ構成を割り当てた後は、ファイルサーバ構成名は変更することができますが、ファイル サーバ自体の変更はできません。
- マネージド ファイル転送がすでに設定済みで、その設定を変更した場合、Cisco XCP Router サービスを再起動すると、マネージドファイル転送機能が再起動します。
- ファイルサーバ自体で設定を変更せずに設定を変更した場合、ファイル転送が機能しなくなり、Cisco XCP Router サービスを再起動するように促す通知が送信されます。
- データベースまたはファイル サーバに障害が発生した場合、その障害を明記するメッセージが生成されます。ただし、エラー応答では、データベースの障害、ファイル サーバの障害、その他の内部障害の内容は区別されません。データベースまたはファイル サーバに障害が発生した場合も、Real-Time Monitoring Tool がアラームを生成します。この警告は、ファイル転送が進行中であるかどうかにかかわらず発せられます。

マネージド ファイル転送の管理の要件

マネージド ファイル転送機能の設定

マネージド ファイル転送管理のタスク フロー

手順

	コマンドまたはアクション	目的
Step 1	AFT_LOG テーブルの SQL クエリの出力例 （321 ページ）	次の手順では、AFT_LOG テーブルで実行できるクエリの例と、その出力を使用してファイル サーバから不要なファイルを削除する方法を説明します。
Step 2	サービス パラメータのしきい値の設定（323 ページ）	マネージドファイル転送サービスパラメータを設定して、外部ファイルサーバーのディスク領域に関する RTMT アラートが生成されるしきい値を定義します。
Step 3	XCP File Transfer Manager のアラームの設定 （323 ページ）	定義されたしきい値に達したことを通知するように、マネージド ファイル転送のアラームを設定します。
Step 4	マネージドファイル転送の外部データベースのクリーンアップ （326 ページ）	オプション。外部データベースのクリーンアップ ユーティリティを使用して、外部

	コマンドまたはアクション	目的
		データベースを監視するジョブを設定し、期限切れのレコードは削除します。これで、常に最新のレコードのために十分なディスク スペースが確保されます。

AFT_LOG テーブルの SQL クエリの出力例

次の手順では、AFT_LOG テーブルで実行できるクエリの例と、その出力を使用してファイル サーバから不要なファイルを削除する方法を説明します。

このクエリは、指定された日付の後にアップロードされた各ファイルのレコードを返します。

（注） SQL コマンド例は、外部データベースのディスク使用量（322 ページ）を参照してください。

手順

Step 1 外部データベースで、次のコマンドを入力します。

```
SELECT file_path
FROM aft_log
WHERE method='Post' AND timestampvalue > '2014-12-18 11:58:39';
```

このコマンドを実行すると、以下の出力が生成されます。

```
/opt/mftFileStore/node_1/files/im/20140811/15/file_name1
/opt/mftFileStore/node_1/files/im/20140811/15/file_name2
/opt/mftFileStore/node_1/files/im/20140811/15/file_name3
/opt/mftFileStore/node_1/files/im/20140811/15/file_name4
...
/opt/mftFileStore/node_1/files/im/20140811/15/file_name99
/opt/mftFileStore/node_1/files/im/20140811/15/file_name100
```

Step 2 rm コマンドとこの出力を使用して、外部ファイルサーバからこれらのファイルを削除するスクリプトを作成します。SQL クエリ例は、*Cisco Unified Communications Manager*での *IM and Presence Service* データベース設定 を参照してください。

（注） ファイルに関連するレコードが外部データベースからすでに消去されていても、そのファイルが外部ファイル サーバからまだ消去されていなければ、そのファイルを引き続きアクセス/ダウンロードできます。

次のタスク

サービス パラメータのしきい値の設定 （323 ページ）

外部データベースのディスク使用量

ディスクやテーブルスペースが満杯にならないようにする必要があります。満杯になると、マネージドファイル転送機能が動作を停止することがあります。以下は、外部データベースからレコードを消去するために使用できる SQL コマンド例です。その他のクエリは、*Cisco Unified Communications Manager*での *IM and Presence Service* データベース設定 を参照してください。

（注） ファイルに関連するレコードが外部データベースからすでに消去されていても、そのファイルが外部ファイル サーバからまだ消去されていなければ、そのファイルを引き続きアクセス/ダウンロードできます。

アクション	コマンド例
アップロードされたファイルのすべてのレコードの削除。	DELETE FROM *aft_log* WHERE *method* = 'Post';
特定のユーザによってダウンロードされたすべてのファイルの削除。	DELETE FROM *aft_log* WHERE *jid* LIKE '<userid>@<domain>%' AND *method* = 'Get';
特定の時刻の後にアップロードされたすべてのファイルのレコードの削除。	DELETE FROM *aft_log* WHERE *method* = 'Post' AND *timestampvalue* > *'2014-12-18 11:58:39';*

さらに、データベースのディスク使用量の管理に便利なカウンタおよび警告があります。詳細については、「マネージド ファイル転送のアラームおよびカウンター （324 ページ）」を参照してください。

サービス パラメータのしきい値の設定

マネージドファイル転送サービスパラメータを設定して、外部ファイルサーバーのディスク領域に関する RTMT アラートが生成されるしきい値を定義します。

手順

Step 1 Cisco Unified CM IM and Presence Administration で、**システム** > **サービス パラメータ**を選択します。

Step 2 ノードの [Cisco XCP File Transfer Manager] サービスを選択します。

Step 3 次のサービス パラメータの値を入力します。

- **外部ファイル サーバの使用可能領域の下限しきい値**：外部ファイル サーバ パーティションで使用可能な領域の割合（%）がこの値以下になると、XcpMFTExtFsFreeSpaceWarn アラームが生成されます。デフォルト値は 10% です。
- **外部ファイルサーバの使用可能領域の上限しきい値**：外部ファイルサーバパーティションで使用可能な領域の割合（%）がこの値以上になると、XcpMFTExtFsFreeSpaceWarn アラームが解除されます。デフォルト値は 15% です。

（注） 下限しきい値を上限しきい値より大きい値に設定しないでください。それ以外の場合、cisco xcp Router サービスを再起動しても、Cisco XCP File Transfer Manager サービスは開始されません。

Step 4 **[保存（Save）]** をクリックします。

Step 5 Cisco XCP Router サービスを再起動します。

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** ドロップダウンから IM and Presence パブリッシャを選択し、**移動**をクリックします。

c) **IM and Presence Services**の下で、**Cisco XCP Router**を選択して、**再起動**をクリックします。

次のタスク

XCP File Transfer Manager のアラームの設定 （323 ページ）

XCP File Transfer Manager のアラームの設定

定義されたしきい値に達したことを通知するように、マネージドファイル転送のアラームを設定します。

手順

Step 1 **Cisco Unified IM and Presence Serviceability**にログインします。

Step 2 **[Alarm（アラーム）] > [Configuration（設定）]** を選択します。

Step 3 **サーバ** ドロップダウンで、サーバ（ノード）を選択して、**移動**をクリックします。

Step 4 **サービス グループ** ドロップダウン リストで、**IM and Presence Services** を選択して、**移動**をクリックします。

Step 5 **サービス** ドロップダウン リストから、**Cisco XCP File Transfer Manager（アクティブ）** を選択して、**移動**を選択します。

Step 6 必要に応じて優先アラーム設定を行います。フィールドとその設定を含むヘルプは、オンラインヘルプを参照してください。

Step 7 **[保存（Save）]** をクリックします。

次のタスク

使用可能な警告およびカウンターの詳細は、以下を参照してください。マネージドファイル転送のアラームおよびカウンター（324 ページ）

マネージド ファイル転送のアラームおよびカウンター

マネージドファイル転送を使用すると、転送されたファイルは、外部ファイルサーバにアーカイブされた後、そして、ファイル メタデータが外部データベースに記録された後にのみ、ユーザに配信されます。IM and Presence Service ノードが外部ファイル サーバまたは外部データベースとの接続を失った場合、 IM and Presence Service は受信者にファイルを配信しません。

マネージド ファイル転送のアラーム

接続が失われた場合に必ず通知されるようにするには、Real-Time Monitoring Tool で以下のアラームが正しく設定されていることを確認します。

（注） 外部ファイル サーバへの接続が失われる前にアップロードされたファイル、およびダウンロード中であったファイルは、受信者へのダウンロードに失敗することになります。ただし、失敗した転送のレコードが外部データベースに残ります。これらのファイルを特定するには、外部データベース フィールド file_size と bytes_transferred の不一致を調べることができます。

表 *31 :* マネージド ファイル転送のアラーム

アラーム	問題	ソリューション
XcpMFTExtFsMountError	Cisco XCP File Transfer Manager で外部ファイル サーバとの接続が失われました。	External File Server Troubleshooter で詳細を確認してください。 外部ファイルサーバーが正常に動作していることを確認します。 外部ファイルサーバーとのネットワーク接続に問題があるかどうか確認します。
XcpMFTExtFsFreeSpaceWarn	Cisco XCP File Transfer Managerは、外部ファイル サーバの空きディスク領域が少ないことを検出しました。	ファイル転送に使われるパーティションから不要なファイルを削除して、外部ファイル サーバの領域を解放します。
XcpMFTDBConnectError	Cisco XCP データ アクセス レイヤがデータベースに接続できませんでした。	システム トラブルシュータで詳細を確認してください。 外部データベースが正常に動作していること、および外部データベース サーバとのネットワーク接続に問題があるかどうか確認します。
XcpMFTDBFullError	ディスクまたはテーブルスペースがいっぱいになっているため、Cisco XCP File Transfer Manager は外部データベースにデータを挿入または変更できません。	データベースを確認し、ディスク領域を解放または回復できるかどうかを評価します。 データベースのキャパシティを追加することを検討してください。

マネージド ファイル転送のカウンター

マネージド ファイル転送を管理しやすくするために、Real-Time Monitoring Tool を介して以下のカウンタを監視することができます。これらのカウンタは、Cisco XCP MFT カウンタ フォルダに保存されます。

表 *32 :* マネージド ファイル転送のカウンター

カウンタ	説明
MFTBytesDownloadedLastTimeslice	このカウンタは、最後のレポート インターバル（通常は 60 秒）の間にダウンロードされたバイト数を表します。
MFTBytesUpoadedLastTimeslice	このカウンタは、最後のレポート インターバル（通常は 60 秒）の間にアップロードされたバイト数を表します。

カウンタ	説明
MFTFilesDownloaded	このカウンタは、ダウンロードされたファイルの総数を表します。
MFTFilesDownloadedLastTimeslice	このカウンタは、最後のレポート インターバル（通常は60秒）の間にダウンロードされたファイル数を表します。
MFTFilesUploaded	このカウンタは、アップロードされたファイルの総数を表します。
MFTFilesUploadedLastTimeslice	このカウンタは、最後のレポート インターバル（通常は60秒）の間にアップロードされたファイル数を表します。

マネージド ファイル転送の外部データベースのクリーンアップ

外部データベースを監視し、期限切れのレコードを削除するジョブを設定します。これで、常に最新のレコードのために十分なディスク スペースが確保されます。

マネージドファイル転送のデータベーステーブルをクリーンアップするには、**[機能テーブル（Feature Tables）]** の下の **[マネージドファイル転送（Managed File Transfer）（MFT）]** 機能が選択されていることを確認します。

手順

Step 1 データベース パブリッシャ ノードで Cisco Unified CM IM and Presence Administration にログインします。

Step 2 **メッセージング** > **外部データベースの設定** > **外部データベース** を選択します。

Step 3 **外部 DB のクリア**をクリックします。

Step 4 次のいずれかを実行します。

- パブリッシャ ノードに接続する外部データベースを手動でクリーンアップするには、**samecup ノード**を選択します。
- サブスクライバ ノードに接続する外部データベースを手動でクリーンアップする場合は、**その他の CupNode** を選択してから、外部データベースの詳細を選択します。
- 外部データベースを自動的にモニタおよびクリーンアップするシステム設定の場合は、**自動クリーンアップ** オプション ボタンをオンにします。

（注） 自動クリーンアップを設定する前に、手動でのクリーンアップを実行することを推奨します。

Step 5 いつまでさかのぼってファイル削除をするかの**日数**を設定します。たとえば、90 を入力した場合、システムは 90 日前以前の古いレコードを削除します。

Step 6 データベースのインデックスとストアドプロシージャを作成するには、**スキーマの更新** をクリックします。

（注）　スキーマの更新は、このジョブを最初に実行するときにのみです。

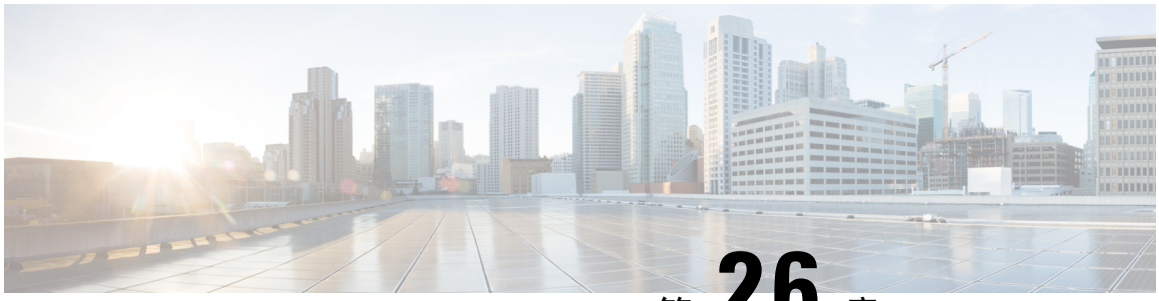
Step 7　いつまでさかのぼってファイル削除をするかの**日数**を設定します。たとえば、**90** を入力した場合、システムは 90 日より前の古いレコードを削除します。

Step 8　**機能テーブル** セクションで、レコードをクリーンアップする各機能を選択します。

- **テキスト会議：**常設チャット機能のデータベース テーブルを消去するには、このオプションを選択します。
- **メッセージアーカイバ（MA）**：メッセージアーカイバ機能のデータベーステーブルをクリーンアップするには、このオプションを選択します。
- **マネージドファイル転送（MFT）：** マネージドファイル転送機能のデータベーステーブルを消去するには、このオプションを選択します。

Step 9　**[クリーンアップジョブを送信（Submit Clean-up Job）]** をクリックします。

（注）　**[自動（Automatic）]** オプションが有効になっていて、それを無効にする場合は、**[自動クリーンアップジョブの無効化（Disable Automatic Clean-up Job）]** ボタンをクリックします。



第 26 章

エンド ユーザの管理

エンド ユーザ管理の概要

IM and Presence Service ノードへユーザを割り当てて、ユーザを IM and Presence Service 用に設定する手順については、以下のガイドを参照してください。

エンド ユーザを管理するための管理タスクの一環として、以下のタスクを管理する必要がある場合があります。

- プレゼンス要求を承認するためのデフォルト ポリシーの設定
- 重複した、あるいは無効なユーザ ID およびディレクトリ URI に対してスケジュールされたシステム チェックの設定
- 問題発生時のユーザ ID およびディレクトリ URI の修正

エンド ユーザのインポートおよび設定方法の詳細は、*Cisco Unified Communications Manager* システム設定ガイドの「エンド ユーザの設定」セクションを参照してください。

ユーザ連絡先リストの一括インポートおよびエクスポートの詳細は、連絡先リストの一括管理（433 ページ）を参照してください。

プレゼンス認証の概要

プレゼンス サブスクリプション要求の場合は、プレゼンス認証ポリシーを割り当てる必要があります。プレゼンス認証ポリシーは、システム レベルで、プレゼンスが要求されているエンド ユーザの認証を要求せずに、システム上のエンド ユーザが他のエンド ユーザのプレゼンス ステータスを表示することができるかどうかを決定します。この設定は、**プレゼンス設定** の設定ウィンドウの **確認プロンプトなしで、ユーザが他のユーザのプレゼンス ステータスを表示できるようにする** チェックボックスで行います。利用できる設定は、展開されたプロトコルに一部左右されます。

- SIP ベースのクライアントの場合、すべてのプレゼンス登録要求を自動的に承認するように IM and Presence Service を設定する必要があります。でないと、プレゼンスは正しく機能しません（これはデフォルト設定です）。このオプションが設定された場合、IM and Presence Service は1つの例外を除いて、すべての要求を自動的に承認します。例外ケースは、プレゼンスが要求されているユーザが、要求を行うユーザを含むブロック リストを Cisco Jabberクライアントに設定している場合です。この場合、ユーザはプレゼンス要求を承認するように促されます。
- XMPP ベースのクライアントの場合は、IM and Presence Service で他のユーザからのプレゼンス要求を許可するようにユーザに要求するかどうか、あるいはそのプレゼンス要求を自動的に許可するかどうかを設定することができます。

（注） 認可システム設定は、エンド ユーザが Cisco Jabber クライアント内で設定可能なユーザ ポリシー設定によって上書きされる場合もあります。

Jabber のユーザ ポリシー設定

プレゼンス要求を承認する際、IM and Presence Service は、ユーザが Cisco Jabber クライアント内で設定したユーザ ポリシーも参照します。エンド ユーザは他のユーザをブロック リストに追加して、他のユーザが許可なしにプレゼンス状態を表示できないようにしたり、許可リストに追加して、自身のプレゼンス状態の表示を許可することができます。これらの設定は、システムのデフォルト設定を上書きします。

エンド ユーザは、Cisco Jabber クライアント内で以下の事項を設定することができます。

- ブロックリスト：ユーザは、他のユーザ（ローカル ユーザと外部ユーザの両方）をブロックリストに追加することができます。ブロックされたユーザのいずれかがそのユーザのプレゼンスを表示した場合、ユーザの実際のステータスとは関係なく、そのユーザの可用性ステータスは常に応対不可として表示されます。ユーザはフェデレーション ドメイン全体を拒否することもできます。
- 許可リスト：ユーザは、他のローカルおよび外部のユーザが常に応対可能性の閲覧を許可することができます。外部（フェデレーション）ドメイン全体を許可することもできます。
- デフォルト ポリシー：ユーザのデフォルト ポリシーの設定。ユーザは、すべてのユーザを拒否するか、すべてのユーザを許可するようにポリシーを設定できます。

ユーザ ID およびディレクトリ URI の検証

単一クラスタ展開の場合、同じクラスタ内で重複するユーザを割り当てることはできないため、重複するユーザ ID およびディレクトリ URIは問題にはなりません。ただし、クラスタ間展開の場合、異なるクラスタの異なるユーザに対して、意図せずに同じユーザ ID またはディレクトリ URI 値を割り当てる可能性があります。

IM and Presence Service は、ユーザ ID およびディレクトリ URI の重複を確認するために、以下の検証ツールを提供します。

- Cisco IM and Presence Data Monitorサービス：このサービスを使用して、継続的なシステム チェックを設定することができます。Cisco IM and Presence Data Monitor サービスは、Active Directory エントリで、すべての IM and Presence Service クラスタの重複ユーザ ID および空または重複ディレクトリ URI をチェックします。管理者は、アラームまたはアラートを介して通知を受けることができます。Cisco Unified Real-Time Monitoring Tool を使用すると、アラームを監視し、重複した UserID および DuplicateDirectoryURI エラーに対して電子メール アラートを設定することができます。
- システムのトラブルシューティング：システムのトラブルシューティングを使用して、ディレクトリ URI およびユーザ ID の重複を含めたシステムのエラーチェックをアドホックに実行する場合は、システムのトラブルシューティングを利用します。トラブル シューティングが詳細を提供するユーザは、最大 10 人までです。システム トラブルシューティングは、Cisco Unified CM IM and Presence の管理インターフェイスからアクセスすることができます（**診断**> **システム トラブルシューティング**を選択します）。
- コマンドライン インターフェイス（CLI）：重複した URI およびユーザ ID の完全で詳細なレポートを入手するには、`utils users validate all` CLI コマンドを実行します。

エンド ユーザ管理のタスク フロー

手順

	コマンドまたはアクション	目的
Step 1	プレゼンス認証ポリシーの割り当て（332 ページ）	プレゼンス サブスクリプション要求用のシステム認証ポリシーを割り当てます。
Step 2	ユーザ データのデータ モニタ チェックの設定 （333 ページ）	Cisco IM and Presence Data Monitor サービスを設定して、重複したディレクトリ URI およびユーザ ID の定期的なチェックを実行します。問題が見つかった場合は、システム アラームまたは警告が発せられます。
Step 3	システム トラブルシューティングを使用したユーザ データの検証 （335 ページ）	重複したディレクトリ URI やユーザ ID など、システムの問題についてアドホックにチェックを実行する場合は、システム トラブルシューティングを実行します。
Step 4	CLI からの ユーザ ID およびディレクトリ URI の検証 （336 ページ）	重複したディレクトリ URI およびユーザ ID の詳細なレポートを取得するには、CLI コマンドを実行します。

	コマンドまたはアクション	目的
Step 5	ユーザのプレゼンス設定の表示（340ページ）	IM and Presence 対応エンド ユーザのプレゼンス設定を表示する必要がある場合は、プレゼンス ビューアを使用して、プレゼンス設定を表示することができます。

プレゼンス認証ポリシーの割り当て

プレゼンス サブスクリプション要求用のシステム認証ポリシーを割り当てます。

（注） Cisco Jabber クライアントで、エンド ユーザは、他のユーザが自分のプレゼンス ステータスを表示できるようにするかどうかを設定することができます。このユーザ ポリシーは、システム認証の設定より優先されます。

手順

Step 1 **Cisco Unified CM IM and Presence管理**で、**プレゼンス** > **設定**を選択します。

Step 2 **確認プロンプトなしで、ユーザが他のユーザのプレゼンスステータスを表示できるようにする**l チェックボックスをオンあるいはオフにします。

- オン：IM and Presence は、ローカル エンタープライズの SIP ベースのクライアントから受信するすべてのプレゼンス登録要求を許可します。
- オフ：IM and Presence は、プレゼンスを要求されたクライアントに対して、すべてのプレゼンス サブスクリプション要求を参照提示します。ユーザは、要求を承認または拒否することができます。

（注） SIP ベースのクライアントを展開している場合は、このチェック ボックスをオンにする必要があります。チェック ボックスをオフのままにした場合、展開はXMPP クライアントのみをサポートします。

Step 3 **[保存（Save）]** をクリックします。

Step 4 Cisco XCP Router サービスを再起動します。

次のタスク

IM and Presence サービスの SIP パブリッシュ トランクの設定に進みます。

ユーザ データのデータ モニタ チェックの設定

スケジュールされた間隔でディレクトリ URI とユーザ ID を検証するように Cisco IM and Presence Data Monitor を設定するには、以下のタスクを実行します。エラーは、すべて Cisco Unified Real-Time Monitoring Tool を使用して、アラームまたは警告を介して伝えられます。

（注） 重複したディレクトリ URI および重複したユーザ ID エラーは、クラスタ間の展開の場合にのみ問題となります。

手順

	コマンドまたはアクション	目的
Step 1	ユーザ ID およびディレクトリ URI 検証チェックのスケジュール設定 （333 ページ）	Cisco IM and Presence Data Monitor チェック用のスケジュールされた間隔を設定します。サービスは、active directory エントリのエラー (ディレクトリ Uri とユーザ Id が重複していないか) を確認します。
Step 2	電子メール アラート用の電子メール サーバの設定 （334 ページ）	オプション。Data Monitor サービスが重複したディレクトリ URI あるいはユーザー ID を検出した際に電子メールで警告を受信したい場合は、Real-Time Monitoring Tool を使用して電子メール サーバを設定する必要があります。
Step 3	電子メール アラートの有効化 （335 ページ）	オプション。DuplicateDirectoryURI および DuplicateUserid アラームの電子メールアラートを有効にするには、以下の手順を実行します。Cisco IM and Presence Data Monitor サービスがこういったアラームのいずれかを返すと、管理者に電子メールが送信されます。

ユーザ ID およびディレクトリ URI 検証チェックのスケジュール設定

Cisco IM and Presence Data Monitor サービスの間隔スケジュールを設定します。このサービスは、重複したディレクトリ URI やユーザ ID を含め、スケジュールされた間隔でデータ エラーをチェックします。このサービスは、エラーが発見されると常に Real-Time Monitoring Tool を介して表示されるアラームまたは警告を発します。

始める前に

Cisco IM and Presence Data Monitor ネットワーク サービスが実行されていなければなりません。デフォルトでは、サービスは実行されています。サービスの実行状況は、Cisco Unified IM and Presence

Serviceability インターフェイスの **[コントロールセンター - ネットワークサービス]** ウィンドウで確認することができます。

手順

Step 1 **Cisco Unified CM IM and Presence管理**で、**システム > サービス パラメータを選択します。**を選択します。

Step 2 **サービス** ドロップダウンで、**Cisco IM and Presence Data Monitor**を選択します。

Step 3 **ユーザ チェック間隔** フィールドに、間隔を分単位で入力します。5 ～ 1440 (分) の整数を入力することができます。デフォルト値は 30 分です。

Step 4 [保存（Save）] をクリックします。

次のタスク

（省略可）DuplicateDirectoryURI または DuplicateUserid alarm が発動した際に電子メール アラートを設定する場合は、電子メール アラート用の電子メール サーバの設定 （334 ページ）

電子メール アラート用の電子メール サーバの設定

Data Monitor の検証チェックでディレクトリ URI およびユーザ ID の重複エラーが見つかった場合は、管理者に電子メールによる警告を受信する設定にすることを推奨します。この設定を行った場合は、このオプションの手順を使用して、電子メールアラート用に電子メールサーバをセットアップします。

手順

Step 1 Real-Time Monitoring Tool のシステム ウィンドウで、[アラート セントラル（Alert Central）] をクリックします。

Step 2 **[システム（System）] > [ツール（Tools）] > [アラート（Alert）] > [電子メール サーバの設定（Config Email Server）]** の順に選択します。

Step 3 [メール サーバ設定（Mail Server Configuration）] ポップアップで、メール サーバの詳細を入力します。

Step 4 **[OK]** をクリックします。

次のタスク

電子メール アラートの有効化 （335 ページ）

電子メール アラートの有効化

DuplicateUserID あるいは DuplicateDirectoryURI システム警告が発せられる際に管理者に電子メールを送信するように Real-Time Monitoring Tool を設定するには、以下の手順を使用します。

始める前に

電子メール アラート用の電子メール サーバの設定 （334 ページ）

手順

Step 1 Real-Time Monitoring Tool の [システム（System）] 領域で、[アラート セントラル（Alert Central）] をクリックします。

Step 2 **IM and Presence** タブをクリックします。

Step 3 電子メール アラートを追加するアラートをクリックします。たとえば、**DuplicateDirecytoryURI** または**DuplicateUserid**システム アラートがあるとします。

Step 4 **ツール** > **アラート** > **アラート アクションの設定**を選択します。

Step 5 [アラート アクション（Alert Action）] ポップアップで、[デフォルト（Default）] を選択して、[編集（Edit）] をクリックします。

Step 6 [アラート アクション（Alert Action）] ポップアップで、受信者を追加します。

Step 7 ポップアップ ウィンドウで、電子メール アラートを送信するアドレスを入力して、[OK] をクリックします。

Step 8 [アラート アクション（Alert Action）] ポップアップで、アドレスが [受信者（Recipients）] に表示されていることと、[有効（Enable）] チェックボックスがオンになっていることを確認します。

Step 9 [OK] をクリックします。

Step 10 電子メールアラートを有効にするシステム アラート毎にこの手順を繰り返します。

システム トラブルシューティングを使用したユーザ データの検証

Cisco Unified CM IM and Presence 管理 GUI でシステム トラブルシューティング を使用することで、重複ユーザ ID および重複ディレクトリ URI チェックのステータスを監視することができます。このトラブル シューティングでは、展開内のすべてのノードおよびクラスタが確認されます。

手順

Step 1 **Cisco Unified CM IM and Presence Administration**で、診断 > **システムのトラブルシューティング**を選択します。

Step 2 ユーザ ID と ディレクトリ URI のステータスを [ユーザ トラブルシュータ（User Troubleshooter）] 領域で監視します。システム チェックで何らかの問題が検出された場合は、**[問題（Problem）]** 列に表示されます。

- すべてのユーザに一意のユーザIDが設定されていることを確認します。
- すべてのユーザにディレクトリ URI が設定されていることを確認します。
- すべてのユーザに一意のディレクトリ URI が設定されていることを確認します。
- すべてのユーザに有効なディレクトリ URI が設定されていることを確認します。
- すべてのユーザに一意のメール ID が設定されていることを確認します。

（注） 重複したメール ID は、フェデレーションと Exchange Calendar の統合機能の両方のメール アドレスに影響を与えます。

Step 3 問題があった場合は、**ソリューション** 列の **修正** リンクをクリックすると、ユーザ設定を再構成することができる Cisco Unified Communications Manager の **エンド ユーザ設定** ウィンドウにリダイレクトされます。

（注） ユーザ プロファイルの [ユーザ ID（User ID）] フィールドと [ディレクトリ URI（Directory URI）] フィールドが LDAP ディレクトリにマップされている場合があります。その場合は、 LDAP ディレクトリ サーバで修正を適用します。

次のタスク

Cisco Unified Communications Manager の [エンド ユーザの設定（End User Configuration）] ウィンドウ。ユーザが LDAP ディレクトリから同期される場合は、LDAP ディレクトリ内で編集を行う必要があります。

より詳細なレポートが必要な場合は、CLI からの ユーザ ID およびディレクトリ URI の検証（336 ページ）。

CLI からの ユーザ ID およびディレクトリ URI の検証

コマンドライン インターフェイスを使用して、ユーザ ID の重複やディレクトリ URI の重複がないか、展開の詳細チェックを実行します。

手順

Step 1 コマンドライン インターフェイスにログインします。

Step 2 次のいずれかのコマンドを実行します。

- `utils users validate all`: 重複ユーザ ID およびディレクトリ URI の両方についてシステムをチェックします。
- `utils users validate userid`: システムでユーザ ID が重複していないかどうかを確認します。

- `utils users validate uri`: システムでディレクトリ URI が重複していないかどうかを確認します。

CLI は、重複したディレクトリ URI および/またはユーザ ID のレポートを返します。レポートの例については、以下を参照してください。ユーザ ID とディレクトリ URI CLI 検証の例（337 ページ）

次のタスク

問題があった場合、Cisco Unified Communications Manager の [エンドユーザの設定ウィンドウ] のユーザ設定を編集します。ユーザが LDAP ディレクトリから同期される場合は、LDAP ディレクトリ内で編集を行う必要があります。

ユーザ ID と ディレクトリ URI CLI 検証の例

重複ユーザ ID と重複または無効なディレクトリ URI が設定されたユーザを識別する IM and Presence サービスのユーザを確認するための CLI コマンドは、utils users validate { all | userid | uri } です。

ディレクトリ URI は、ユーザ毎に一意である必要があります。複数のユーザに同じディレクトリ URI を使用することはできません。大文字と小文字の違いがある場合でも、使用できません。たとえば、`aaa@bbb.ccc`と `AAA@BBB.CCC`のように、大文字と小文字の違いはあっても、これらで 2 つの異なるディレクトリ URI を作成することはできません。

CLI とコマンドの説明の使用方法の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

ユーザ ID エラーを表示する CLI 出力例

```
Users with Duplicate User IDs
---------------------------------------------
 User ID: user3
  Node Name
  cucm-imp-1
  cucm-imp-2
```

ディレクトリ URI エラーを表示するCLI 出力例

```
Users with No Directory URI Configured
-----------------------------------------------------
 Node Name: cucm-imp-2
 User ID
 user4

Users with Invalid Directory URI Configured
-----------------------------------------------------
 Node Name: cucm-imp-2
 User ID   Directory URI
 user1     asdf@ASDF@asdf@ADSF@cisco

Users with Duplicate Directory URIs
-----------------------------------------------------
```

```
Directory URI: user1@cisco.com
 Node Name   User ID
 cucm-imp-1  user4
 cucm-imp-2  user3
```

ユーザ IDおよび ディレクトリ URI エラー

Cisco IM and Presence Data Monitor サービスは、Active ディレクトリ エントリで、すべての IM and Presence Service クラスタの重複ユーザ ID および空または重複ディレクトリ URI をチェックします。重複ユーザ ID またはディレクトリ URI はクラスタ内では無効です。ただし、誤ってクラスタ間展開の異なるクラスタのユーザに同じユーザ ID または ディレクトリ URI 値を割り当てる可能性があります。

以下は、検出される可能性のあるエラーを提示しています。これらのエラーはReal-Time Monitoring Tool で確認することができます。Real-Time Monitoring Tool では、以下の各設定についてアラームあるいは警告が発せられます。

DuplicateDirectoryURI

このアラートは、ディレクトリ URI IM アドレス スキームが設定されている時、同じディレクトリ URI 値が割り当てられているクラスタ間展開内に複数のユーザが設定されていることを示します。

DuplicateDirectoryURIWarning

この警告は `userID@ Default_Domain` IM アドレス スキームが設定されている時に、同じディレクトリ URI 値が割り当てられているクラスタ間展開内に複数のユーザが設定されていることを示します。

DuplicateUserid

このアラートは、クラスタ間展開内の別のクラスタで 1 人以上のユーザに割り当てられた重複ユーザ ID が設定されていることを示します。

InvalidDirectoryURI

この警告は、ディレクトリ URI IM アドレス スキームが設定されている時、クラスタ間展開内の 1 つ以上のユーザに空または無効なディレクトリ URI 値が割り当てられていることを示します。

InvalidDirectoryURIWarning

このアラートは `userID@Default_Domain` IM Adress スキームが設定されている時、クラスタ間展開内の 1 つ以上のユーザに空または無効な ディレクトリ URI 値が割り当てられていることを示します。

これらのアラーム条件に関連するユーザの特定情報を収集するには、Command Line Interface を使用して、その完全な一覧を確認してください。システム アラームは、影響を受けるユーザの詳細を提供しません。また、システム トラブルシュータは最大で10ユーザのみの詳細を表示します。Command Line Interface を使用してユーザを確認し、アラームが発生しているユーザに関する情報を収集します。詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

⚠

注意　影響を受けているユーザの通信の中断を避けるために、重複ユーザIDおよび重複しているか無効なディレクトリ URI を解決するための適切な処置をとります。ユーザの連絡先情報を変更するには、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

エラーおよび推奨操作

次の表は、重複ユーザおよび重複または無効なディレクトリ URI のシステム確認をクラスタ間展開で実行するときに起こる可能性のあるユーザIDとディレクトリURIのエラー状態を示します。発生するアラームとそのエラーを修正するための推奨措置が一覧表示されます。

表 *33*：ユーザ *ID* と ディレクトリ *URI* のエラー状態および推奨される処置

エラー状態	説明	推奨措置
重複ユーザ ID	重複ユーザ ID は、クラスタ間展開内で別のクラスタの 1 人以上のユーザに割り当てられます。影響を受けるユーザが、クラスタ間ピアに配置されている場合があります。 **関連アラーム：** `DuplicateUserid`	`DuplicateUserid` アラートが発生したら、問題を修正するために即時に対処してください。クラスタ間展開内の各ユーザは一意なユーザ ID が必要です。
重複したディレクトリ URI	クラスタ間展開内の複数のユーザに同じディレクトリ URI 値が割り当てられます。影響を受けるユーザが、クラスタ間ピアに配置されている場合があります。 **関連アラーム：** • `DuplicateDirectoryURI` • `DuplicateDirectoryURIWarning`	ディレクトリ URI IM アドレススキームを使用するようにシステムが設定がされていて、`DuplicateDirectoryURI` アラートが発生した場合、問題を修正するために即時に対処をしてください。各ユーザは一意のディレクトリ URI が割り当てられる必要があります。 *userID@Default_Domain* IM アドレススキームを使用するように設定されていて、重複ディレクトリ URI が 検出されると、`DuplicateDirectoryURIWarning` の警告が発生します。即時に対処する必要はありませんが、問題を解決することを推奨します。

エラー状態	説明	推奨措置
無効なディレクトリ URI	展開内の1人以上のユーザに無効または空のディレクトリ URI 値が割り当てられます。*user@domain* 形式でない URI は無効なディレクトリ URI です。影響を受けるユーザが、クラスタ間ピアに配置されている場合があります。 **関連アラーム:** • `InvalidDirectoryURI` • `InvalidDirectoryURIWarning`	ディレクトリ URI IM アドレススキームを使用するように設定がされていて、次のアラートが発生した場合、問題を修正するために即時に対処します。`InvalidDirectoryURI`。 *userID@Default_Domain* IM アドレススキームを使用するための設定がされており、無効なディレクトリ URI が検出された場合、`InvalidDirectoryURIWarning` の警告が発生します。即時に対処する必要はありませんが、問題を解決することを推奨します。

ユーザのプレゼンス設定の表示

プレゼンス ビューアを使用して、IM and Presence が有効なエンドユーザのプレゼンス設定の概要を確認することができます。プレゼンス ビューアは、プレゼンス サーバの割り当て、連絡先、ウォッチャーなどの情報を提供します。

始める前に

Cisco **AXL Web サービス、Cisco SIP Proxy** サービス、および**Cisco Presence Engine** サービスは、すべて Cisco Unified Serviceabilityで実行されていなければなりません。

手順

Step 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] **[ユーザの管理（User Management）]** > **[エンド ユーザ（End Users）]** を選択します。

Step 2 **検索** をクリックして、新しい電話機を追加するユーザを選択します。

Step 3 **サービス設定**の下の**ユーザのプレゼンス ビューア**をクリックして、プレゼンス ビューアを開きます。ビューをカスタマイズする場合は、以下の表を参照してください。

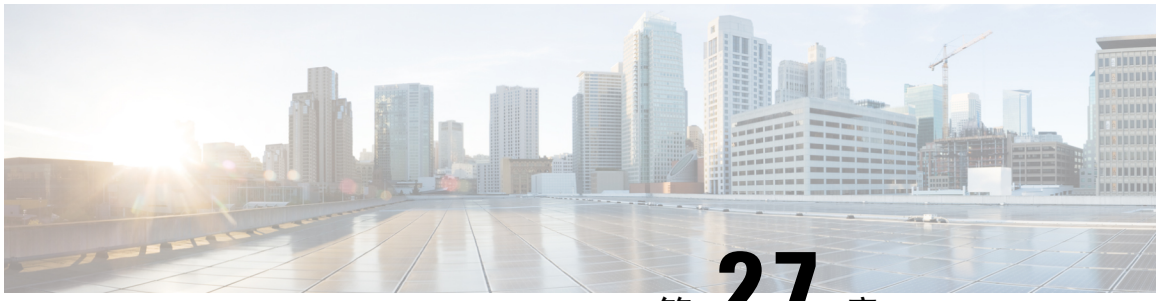
表 *34 :* エンド ユーザ プレゼンス ビューアのフィールド

プレゼンス設定	**[説明（Description）]**
[User Status]	ユーザのプレゼンス ステータスを特定します。ステータスには、以下があります。 • 使用可能 • 退席中 • サイレント • 使用不可 • Custom
ユーザー ID	選択したユーザ ID を識別します。ユーザの写真を使用できる場合は、ユーザの写真が表示されます。 別のユーザ ID を選択するには、**送信** をクリックします。
以下の視点での表示	ユーザの視点から応答可能性のステータスを表示するユーザを指定します。これで、指定したユーザーの応答可能性のステータスがウォッチャと呼ばれる別のユーザーにどのように表示されるかを判断することができます。この機能は、たとえば、ユーザがプライバシー ポリシーを設定している場合のデバッグ シナリオで役立ちます。 最大 128 文字を使用できます。
連絡先	このユーザの連絡先リストにある連絡先の数が表示されます。 特定のユーザ連絡先の応答可能性のステータスを表示するには、[連絡先およびウォッチャ] リスト領域の [連絡先] 見出しの横にある矢印をクリックします。グループ名の横の矢印をクリックして、そのグループ内の連絡先のリストを展開します。 グループに属していない連絡先は、連絡先グループリストの下に表示されます。1つの連絡先が複数のグループに所属している場合は、そのユーザの連絡先リストのサイズに対してカウントされるのは一度だけです。 エンドユーザに対して設定されている連絡先の最大数を超えると、警告メッセージが表示されます。IM and Presence Service の設定および連絡先の最大設定の詳細は、*IM and Presence* 管理 オンライン ヘルプを参照してください。

プレゼンス設定	[説明（**Description**）]
ウォッチャ（Watchers）	連絡先リストでこのユーザーの応答可能性のステータスを確認するためにサブスクライブしているウォッチャと呼ばれるユーザのリストを表示します。 特定のウォッチャの応答可能性のステータスを表示するには、[連絡先およびウォッチャ] リスト領域の [ウォッチャ] 見出しの横にある矢印をクリックします。グループ名の横にある矢印をクリックして、そのグループ内のウォッチャのリストを展開します。 ウォッチャは複数のグループに属することができますが、そのユーザのウォッチャのリストサイズに対してカウントされるのは一度だけです。 エンドユーザ用に設定されているウォッチャの数が上限を超えると、警告メッセージが表示されます。IM and Presence Service の設定およびウォッチャの最大設定の詳細は、 *IM and Presence* 管理オンラインヘルプを参照してください。
プレゼンス サーバの割り当て	ユーザが割り当てられている IM and Presence Service サーバを識別します。ハイパーリンクを使用すると、サーバの設定ページに直接移動して、詳細を確認することができます。
アクセス可能なプレゼンス アイコンの有効化	このチェックボックスをオンにすると、このエンドユーザのプレゼンス アクセシビリティ アイコンが有効となります。
送信	プレゼンスビューアーを実行する場合に選択します。 有効なプレゼンス情報を取得するには、ユーザを IM and Presence ノードに割り当てる必要があります。この機能を実行するには、AXL、プレゼンス エンジン、およびプロキシサービスが IM and Presence サーバ上で実行されている必要があります。

BLF プレゼンスの連携動作と制限事項

機能	制限事項
自動プレゼンス認証の無効化	プレゼンス要求の自動認証をオフにした場合でも、IM and Presence サービスは他のユーザの連絡先リストにあるユーザの登録要求を自動的に許可することに留意します。これは、同じドメイン内のユーザおよび異なるドメイン内のユーザ（フェデレーション ユーザ）に適用されます。例： • ユーザ A が、ユーザ B の返答可能性状況の表示を登録することを望んでいます。自動承認は IM and Presence サービスでオフになっており、ユーザ B はユーザ A の許可リストまたはブロックリストにないとします。 • IM and Presence Serviceはユーザ B のクライアント アプリケーションにプレゼンス登録要求を送信し、クライアント アプリケーションは登録を許可または拒否するようにユーザ B に求めます。 • ユーザ B は、プレゼンス登録要求を受け入れ、ユーザ B はユーザ A の連絡先リストに追加されます。 • ユーザ A は、プレゼンス登録を許可するように求められることなく、ユーザ B の連絡先リストに自動的に追加されます。これは、ユーザ B のポリシーが外部ドメインをブロックしている場合、またはユーザ Bがユーザー プロファイルで 「 ask me 」 を構成している場合でも発生します。
ドメイン間フェデレーション：外部ドメインから受信したプレゼンス要求	IM and Presence は、プレゼンス ステータスが要求されたユーザのユーザポリシー設定にのみ依存します。ユーザがユーザポリシーで [確認する] を選択していて、そのユーザが外部連絡先またはドメインに対して許可または拒否リストを追加していない場合、IM and Presence はエンド ユーザにプレゼンス要求を送信して承認を待ちます。



第 27 章

ユーザの中央展開への移動

ユーザの中央展開への移動の概要

この章では、既存の IM およびプレゼンスサービスを使用しているユーザを標準の分散 IM およびプレゼンスサービスの導入 (Cisco Unified Communications Manager IM and Presence サービス) から展開に移行する手順について説明します。集中展開では、IM and Presence 展開とテレフォニー展開は、別々のクラスタに位置します。

中央クラスタ マイグレーションの要件となるタスク

すべてのユーザを既存の分散クラスタから移行させる新たな IM and Presence 中央クラスタを設定する場合は、以下の必須手順を実行して、移行用クラスタを設定します。

（注） 移行に含まれない新しいユーザを追加する場合は、集中展開の設定 （115 ページ）の手順に従って、新しいユーザに中央クラスタを設定することができます。設定が正常に動作していることを確信した後にのみ、既存のユーザを中央クラスタに移行します。

表 *35*：移行前のタスク

	移行前のタスク
ステップ 1	新しい中央クラスタを移行クラスタに接続します。 **1.** IM and Presence サービスの集中型クラスタでデータベース パブリッシャ ノードにログインします。 **2.** Cisco Unified CM IM and Presence Administration から、**[システム（System）]** > **[集中展開（Centralized Deployment）]** を選択します。 **3.** [検索**(Find)**] をクリックして、次のいずれかを実行します。 • 既存のクラスタを選択して、**選択したものを編集する** をクリックします。 • [**新規追加（Add New）**] をクリックして、移行クラスタを追加します。 **4.** 追加する移行クラスタ毎に、以下のフィールドに入力を行います。 • **ピア アドレス(Peer Address)**：リモート テレフォニーのパブリッシャ ノードの FQDN、ホスト名、IPv4 アドレス、または IPv6 アドレス • **AXL ユーザ名(AXL Username)**：リモート クラスタ上の AXL アカウントのログイン ユーザ名。 • [AXLパスワード（AXL Password）]：リモート クラスタ上の AXL アカウントのパスワード。 **5. [保存（Save）]** をクリックします。
ステップ 2	新しい中央クラスタが IM and Presence クラスタ間ネットワークの一部になる場合は、中央クラスタと、移行の一部ではない IM and Presence ピアクラスタ間のクラスタ間ピアリングを設定します。次のガイドラインが適用されます。 • 中央クラスタと移行クラスタ間でクラスタ間ピアリングを設定する必要はありません。ただし、移行しているクラスタに、移行時に任意の数の非移行クラスタが設定されているクラスタ間ピア接続がある場合は、これらのクラスタ間ピア接続が中央クラスタで設定されている必要があります。移行または移行は機能しません。 • クラスタ間ピアリングを設定した後は、クラスタ間ピアリングステータスを確認して、設定が正しく機能することを確認してください。 詳細については、クラスタ間ピアの設定 （183 ページ）を参照してください。

中央クラスタ タスク フローへの移行

これらのタスクを実行して、既存のユーザを分散クラスタ（Cisco Unified Communications Manager IM and Presence サービス）から中央管理の IM and Presence クラスタに移行します。このタスク フローに含まれるタスク：

- **IM and Presence Central Cluster** は、ユーザの移行先クラスタを参照します。移行後は、このクラスタは IM and Presence のみを処理します。
- **移行元 クラスタ**とは、IM and Presence ユーザの移行元 クラスタを指します。このクラスタは移行後は、テレフォニーのみを処理します。

はじめる前に

IM and Presence の中央クラスタが新たにインストールされたクラスタであり、まだユーザを持っていない場合は、ユーザを移行する前に中央クラスタマイグレーションの要件となるタスク（345 ページ）を完了します。

表 *36 :* 中央クラスタ タスク フローへの移行

	IM and Presence 中央クラスタ	クラスタの移行	目的
ステップ 1		移行元クラスタからの連絡先リストのエクスポート（349 ページ）	移行クラスタのユーザ連絡先リストを csv ファイルにエクスポートします。
ステップ 2		移行元クラスタのハイ アベイラビリティの無効化（350 ページ）	移行元クラスタ内のすべてのプレゼンス冗長グループ（サブクラスタ）のハイ アベイラビリティを無効にします。
ステップ 3		IM and Presence の UC Service の設定 （351 ページ）	移行元クラスタで、IM and Presence 中央クラスタをポイントする IM and Presence UC サービスを設定します。
ステップ 4		IM and Presence のサービス プロファイルの作成 （352 ページ）	移行元クラスタで、設定した IM and Presence UC サービスを使用するサービス プロファイルを作成します。
ステップ 5		テレフォニー クラスタでのプレゼンス ユーザの無効化（352 ページ）	移行元クラスタの一括管理を使用して、ユーザの IM and Presence を無効にします。

	IM and Presence 中央クラスタ	クラスタの移行	目的
ステップ 6		中央クラスタの OAuth 認証を有効にする（354ページ）	オプション。移行元クラスタで、OAuth 更新ログインを有効にします。これで、中央クラスタの機能も有効になります。
ステップ 7	中央クラスタのハイ アベイラビリティの無効化（354ページ）		IM and Presence 中央クラスタのすべてのプレゼンス冗長グループ（サブクラスタ）でハイ アベイラビリティを無効にします。
ステップ 8	中央および移行クラスタのピア関係を削除する（355ページ）		クラスタ間ピアリングが中央クラスタと移行クラスタの間に存在する場合は、両方のクラスタでピア接続を削除します。
ステップ 9	Cisco Intercluster Sync Agent（356 ページ）		IM and Presence 中央クラスタ内の Cisco Intercluster Sync Agent を停止します。
ステップ 10	機能グループ テンプレート経由の IM and Presence の有効化（356 ページ）		中央クラスタで、IM and Presence サービスを有効にする機能グループ テンプレートを設定します。
ステップ 11	中央クラスタでの LDAP 同期の完了（357 ページ）		LDAP ディレクトリ同期への機能グループ テンプレートの追加移行元クラスタから、この同期を使用して、ユーザを追加します。
ステップ 12	中央クラスタへの連絡先リストのインポート（359ページ）		一括管理と、前の手順で作成した csv エクスポート ファイルを使用して、連絡先リストを中央クラスタにインポートします。
ステップ 13	Cisco Intercluster Sync Agent を起動する（360 ページ）		中央クラスタで Cisco Intercluster Sync Agent を起動します。

	IM and Presence 中央クラスタ	クラスタの移行	目的
ステップ 14	中央クラスタのハイ アベイラビリティの有効化 （360 ページ）		中央クラスタ内のすべてのプレゼンス冗長グループでハイ アベイラビリティを有効にします。
ステップ 15	移行クラスタの残りのピアを削除する （361 ページ）		移行クラスタ (現在はテレフォニークラスタ) とその他のピアクラスタ間の残りのクラスタ間ピア接続を削除します。

移行元クラスタからの連絡先リストのエクスポート

この手順は、分散 IM and Presence 展開から集中配置に移行する場合にのみ使用します。移行元クラスタで、ユーザの連絡先リストを csv ファイルにエクスポートして、後で中央クラスタにインポートします。以下の 2 種類の連絡先リストをエクスポートすることができます。

- 連絡先リスト：このリストは、IM and Presence 連絡先で構成されます。IM アドレスがない連絡先は、このリストにエクスポートされません（非プレゼンス連絡先リストをエクスポートする必要があります）。
- 非プレゼンス連絡先リスト：このリストは、IM アドレスを持っていない連絡先で構成されます。

手順

Step 1 古いクラスタ（テレフォニークラスタ）で Cisco Unified CM のIM and Presence 管理にログインします。

Step 2 エクスポートする連絡先リストの種類に応じて、以下のいずれかのオプションを選択します。

- 連絡先リストのエクスポートは、**一括管理(Bulk Administration)** > **連絡先リスト(Contact List)** > **連絡先リストのエクスポート(Export Contact List)**を選択します。
- 非プレゼンス連絡先リストのエクスポートの場合は、**一括管理(Bulk Administration)** > **非プレゼンス連絡先リスト(Non-presence Contact List)** > **非プレゼンス連絡先リストのエクスポート(Export Non-presence Contact List)** を選択し、次のステップはスキップします。

Step 3 連絡先リストのみ。連絡先リストをエクスポートするユーザを選択します。

a) **連絡先リストのオプションのエクスポート**の下で、連絡先リストのエクスポート先となるユーザのカテゴリを選択します。デフォルトのオプションは**クラスタ内のすべてのユーザ**です。

b) **検索(Find)** をクリックして、ユーザ リストを表示して、**次へ(Next)** をクリックします。

Step 4 **ファイル名** を入力します。

Step 5 **ジョブ情報** の下で、このジョブをいつ実行するかを設定します。

- **すぐに実行**：連絡先のリストを即座にエクスポートするには、このボタンをオンにします。
- **後で実行**：ジョブを実行する時間をスケジュールする場合は、このボタンをオンにします。

Step 6 [送信（Submit）] をクリックします。

（注） **すぐに実行**を選択した場合、エクスポート ファイルは即時に生成されます。**後で実行する**を選択した場合は、このジョブを実行する時間をスケジュールするために、（**一括管理**>**ジョブ スケジューラ**）でジョブ スケジューラを使用しなければなりません。

Step 7 エクスポート ファイルが生成された後のCSV ファイルのダウンロード：

a) **一括管理(Bulk Administration)**>**ファイルをアップロード/ダウンロード(Upload/Download Files)** を選択します。
b) [検索（Find）] をクリックします。
c) ダウンロードするエクスポート ファイルを選択して、**選択したファイルをダウンロード** をクリックします。
d) 安全性の高い場所にファイルを保存します。

Step 8 別のCSVエクスポートファイルを作成する場合は、この手順を繰り返します。たとえば、連絡先リストのエクスポート ファイルを作成する場合は、非プレゼンスの連絡先リストとして別のファイルを作成することができます。

次のタスク

移行元クラスタのハイ アベイラビリティの無効化 （350 ページ）

移行元クラスタのハイ アベイラビリティの無効化

集中展開型への移行の場合は、移行元テレフォニー クラスタの各プレゼンス冗長グループ（サブクラスタ）でハイ アベイラビリティを無効にします。

（注） [**プレゼンス冗長グループの詳細**]ページには、クラスタで高可用性が無効になっている場合でも、すべてのアクティブな JSM セッションが表示されます。

手順

Step 1 古いクラスタで、Cisco Unified Communications Manager のパブリッシャ ノードにログインします

Step 2 Cisco Unified CM Administration から、**[システム（System）]**>**[プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。

Step 3 **検索(Find)** をクリックします。

Step 4 **ハイ アベイラビリティの有効化**のチェック ボックスをオフにします。

Step 5 **[保存（Save）]** をクリックします。

Step 6 サブクラスタ毎に、この手順を繰り返します。

（注） すべてのサブクラスタに対してこの手順を完了したら、少なくとも2分待ってから、このクラスタで追加の設定を完了に進みます。

次のタスク

IM and Presence の UC Service の設定 （351 ページ）

IM and Presence の UC Service の設定

リモート テレフォニー クラスタでこの手順を使用して、IM and Presence サービスの中央クラスタを指す UC サービスを設定します。テレフォニー クラスタのユーザは、IM and Presence 集中クラスタから IM and Presence サービスを取得します。

手順

Step 1 テレフォニー クラスタで Cisco Unified CM の管理インターフェイスにログインします。

Step 2 **[ユーザ管理（User Management）]** > **[ユーザ設定（User Settings）]** > **[UCサービス（UC Service）]** を選択します。

Step 3 次のいずれかを実行します。

a) [検索（Find）] をクリックし、編集する既存のサービスを選択します。

b) [新規追加（Add New）] をクリックして、新しい UC サービスを作成します。

Step 4 [UCサービスタイプ（UC Service Type）] ドロップダウン リスト ボックスから、[IM and Presence] を選択し、[次へ（Next）] をクリックします。

Step 5 [製品タイプ（Product type）] ドロップダウン リスト ボックスから、[IM and Presenceサービス（IM and Presence Service）] を選択します。

Step 6 クラスタの一意の [名前（Name）] を入力します。これはホスト名である必要はありません。

Step 7 **ホスト名 / IP アドレス**で、IM and Presence の集中型クラスタ データベース のパブリッシャ ノードのホスト名、IPv4 アドレス、あるいは IPv6 アドレス を入力します。

Step 8 **[保存（Save）]** をクリックします。

Step 9 推奨。この手順を繰り返して、**ホスト名 / IP アドレス** フィールドが集中クラスタのサブスクライバ ノードを指す 2 番目の IM and Presence サービスを作成します。

次のタスク

IM and Presence のサービス プロファイルの作成 （352 ページ）

IM and Presence のサービス プロファイルの作成

リモート テレフォニー クラスタでこの手順を使用して、IM and Presence 中央クラスタを指すサービス プロファイルを作成します。テレフォニー クラスタのユーザは、このサービス プロファイルを使用して中央クラスタから IM and Presence サービスを取得します。

手順

Step 1 Cisco Unified CM の管理から、**[ユーザ管理（User Management）]** > **[ユーザ設定（User Settings）]** > **[サービスプロファイル（Service Profile）]** を選択します。

Step 2 次のいずれかを実行します。

a) [検索（Find）] をクリックし、編集する既存のサービス プロファイルを選択します。

b) [新規追加（Add New）] をクリックして、新しいサービス プロファイルを作成します。

Step 3 **IM and Presence Profile** セクションで、以前のタスクで設定した IM and Presence サービスを設定します。

a) **プライマリ** ドロップダウンでデータベース パブリッシャ ノード サービスを選択します。

b) **セカンダリ** ドロップダウンで、サブスクライバ ノード サービスを選択します。

Step 4 [保存（Save）] をクリックします。

次のタスク

テレフォニー クラスタでのプレゼンス ユーザの無効化 （352 ページ）

テレフォニー クラスタでのプレゼンス ユーザの無効化

テレフォニー展開で既に LDAP 同期が完了している場合は、一括管理ツールを使用して、IM and Presence ユーザのテレフォニー クラスタ内のユーザ設定を編集します。この設定では、プレゼンス ユーザが IM and Presence サービス の集中クラスタを指します。

（注） この手順は、テレフォニークラスタのLDAP同期がすでに完了していることを前提としています。ただし、LDAP の初期同期が未完了の場合は、最初の同期にプレゼンス ユーザの集中導入設定を追加することができます。この場合は、テレフォニー クラスタに対して以下の操作を実行します。

- 先ほど設定した**サービス プロファイル**を含む機能グループテンプレートを設定します。**ホーム クラスタ** オプションが選択されていること、**Unified CM IM and Presence のユーザを有効にする** オプションが選択されていないことを確認してください。
- **LDAP ディレクトリ設定**で、**機能グループ テンプレート** を LDAP ディレクトリ同期に追加します。
- 最初の同期を完了します。

機能グループ テンプレートおよび LDAP ディレクトリ同期の設定の詳細は、*Cisco Unified Communications Manager*システム設定ガイドの「エンド ユーザの設定(Configure End Users)」セクションを参照してください。

手順

Step 1 Cisco Unified CM Administration で、**クエリ(Query)** > **一括管理(Bulk Administration)** > **ユーザ(Users)** > **ユーザの更新(Update Users)** > **クエリ(Query)**を選択します。

Step 2 フィルタで、**ホーム クラスタが有効(Home Cluster Enabled)**を選択し、**検索(Find)**をクリックします。このウィンドウには、ここをホームクラスタとするすべてのエンドユーザが表示されます。

Step 3 [次へ（Next）] をクリックします。
ユーザ設定の更新 ウィンドウの一番左のチェックボックスで、この設定をこのクエリで編集するかどうかが表示されます。左側のチェック ボックスをチェックしないと、フィールドはクエリによって更新されません。右側のフィールドは、このフィールドの新しい設定を示しています。2 つのチェックボックスが表示されている場合は、左側のチェックボックスをオンにしてフィールドを更新し、右側のチェック ボックスには新しい設定を入力する必要があります。

Step 4 **サービスの設定**で、以下の各フィールドの左側のチェックボックスをオンにして、これらのフィールドを更新することを示してから、隣の設定を以下に従って編集します。

- **ホーム クラスタ**：ホーム クラスタとしてテレフォニー クラスタを有効にするには、右側のチェック ボックスをオンにします。
- **Unified CM IM and Presence のユーザを有効にする**：右のチェックボックスはオンにしません。この設定では、IM and Presenceのプロバイダーとしてテレフォニー クラスタを無効にします。
- **UC サービス プロファイル**—ドロップ ダウンから、先ほどのタスクで設定したサービス プロファイルを選択します。この設定では、IM およびプレゼンスサービス のプロバイダーとなる IM and Presenceの集中クラスタがユーザに表示されます。

（注） Expressway モバイルおよびリモートアクセスの設定については、https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.htmlにある『*Cisco Expressway* 経由のモバイルおよびリモートアクセス導入ガイド』を参照してください。

Step 5 残りのすべてフィールドの入力を完了します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

Step 6 **ジョブ情報**の下の**今すぐ実行(Run Immediately)**を選択します。

Step 7 [Submit] をクリックします。

次のタスク

中央クラスタの OAuth 認証を有効にする （354 ページ）

中央クラスタの OAuth 認証を有効にする

テレフォニー クラスタの OAuth 認証を有効にするには、以下の手順を使用します。これで、IM and Presence 中央クラスタでも OAuth 認証が可能になります。

手順

Step 1 テレフォニー クラスタで Cisco Unified CM 管理にログインします。

Step 2 **システム** > **エンタープライズ パラメータ**を選択する

Step 3 **SSO と OAuth の設定** の下で、**更新ログイン フローを使用した OAuth** のエンタープライズ パラメータを **有効**に設定します。

Step 4 パラメータ設定を編集した場合は、**保存**（**Save**）をクリックします。

中央クラスタのハイ アベイラビリティの無効化

IM and Presence 中央クラスタの各プレゼンス冗長グループ（サブクラスタ）でハイ アベイラビリティが無効であることを確認します。この手順は、設定の適用またはユーザの移行を開始する前に行う必要があります。

（注） [**プレゼンス冗長グループの詳細**]ページには、クラスタで高可用性が無効になっている場合でも、すべてのアクティブな JSM セッションが表示されます。

手順

Step 1 中央クラスタの Cisco Unified CM 管理インスタンスにログインします。

Step 2 **[System（システム）] > [Presence Redundancy Groups（プレゼンス冗長グループ）]** を選択します。

Step 3 **検索(Find)** をクリックして、既存のサブ クラスタを選択します。

Step 4 **ハイ アベイラビリティの有効化**のチェック ボックスをオフにします。

Step 5 **[保存（Save）]** をクリックします。

Step 6 各サブ クラスタに対してこの手順を繰り返します。

次のタスク

Cisco Intercluster Sync Agent （356 ページ）

中央および移行クラスタのピア関係を削除する

IM and Presence 中央クラスタと移行クラスタの間にクラスタ間ピアリングが存在する場合は、そのピア関係を削除します。

手順

Step 1 IM and Presence サービス の中央クラスタのパブリッシャ ノードにログインします。

Step 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。

Step 3 **検索(Find)** をクリックして移行クラスタを選択します。

Step 4 [削除（Delete）] をクリックします。

Step 5 **Cisco XCP ルータ**を再起動します:

a) Unified IM and Presence Serviceability にログインして、**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。

b) **サーバ** リストから、データベース パブリッシャ ノードを選択して、**移動(Go)**をクリックします。

c) [IM and Presenceサービス（IM and Presence Services）] の下で、[Cisco XCPルータ（Cisco XCP Router）] を選択し、[リスタート(Restart)] をクリックします

Step 6 移行クラスタでこれらの手順を繰り返します。

Cisco Intercluster Sync Agent

IM and Presence の中央クラスタを設定する前に、中央クラスタで**Cisco Intercluster Sync Agent**サービスが停止していることを確認します。

手順

Step 1 Cisco Unified IM and Presence のサービスアビリティから、**ツール > コントロールセンタ - ネットワークサービス**を選択します。

Step 2 **サーバ** ドロップダウン リスト ボックスからパブリッシャ ノードを選択し、**移動(Go)** をクリックします。

Step 3 **Cisco Intercluster Sync Agent** のステータスを確認します。サービスが開始されているか、アクティブである場合は、隣接するオプション ボタンを選択して、**停止(Stop)**をクリックします。

次のタスク

機能グループ テンプレート経由の IM and Presence の有効化 （356 ページ）

機能グループ テンプレート経由の IM and Presence の有効化

この手順で、集中クラスタの IM and Presence の設定を使用して機能グループ テンプレートを設定します。機能グループ テンプレートを LDAP ディレクトリの設定に追加して、同期ユーザに IM and Presence を設定することができます。

（注） 初回同期がまだ行われていない場合にのみ、LDAP ディレクトリ同期に機能グループ テンプレートの編集内容を適用することができます。集中クラスタから LDAP 設定を同期した後は、Cisco Unified Communications Manager の LDAP 設定に編集を適用することはできません。すでにディレクトリを同期している場合は、一括管理を使用して、ユーザの IM and Presence を設定する必要があります。詳細については、「一括管理を介した IM and Presence ユーザの有効化（125 ページ）」を参照してください。

手順

Step 1 IM and Presence 集中型クラスタの Cisco Unified CM の管理インターフェイスにログインします。このサーバにはテレフォニーが設定されていてはいけません。

Step 2 **[ユーザ管理（User Management）] > [ユーザ電話/追加（User Phone/Add）] > [機能グループテンプレート（Feature Group Template）]** を選択します。

Step 3 次のいずれかを実行します。

- [検索（Find）] をクリックし、既存のテンプレートを選択します。

- [新規追加（Add New）] をクリックして新しいテンプレートを作成します。

Step 4 次の両方のチェックボックスをオンにします。

- **[ホームクラスタ（Home Cluster）]**
- **[Unified CM IM and Presence のユーザを有効にする（Enable User for Unified CM IM and Presence）]**

Step 5 [機能グループ テンプレートの設定（Feature Group Template Configuration）] ウィンドウの残りのフィールドに入力します。フィールドとその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。

Step 6 [保存（Save）] をクリックします。

次のタスク

設定をユーザに適用するには、初期同期がまだ行われていない場合は、機能グループ テンプレートを LDAP ディレクトリの設定に追加してから初期同期を完了する必要があります。

中央クラスタでの LDAP 同期の完了 （357 ページ）

中央クラスタでの LDAP 同期の完了

リモート Cisco Unified Communications Manager のテレフォニー クラスタでこの手順を使用して、LDAP 同期を使用して、IM and Presence 集中型設定を Ciscoユニファイド コミュニケーション マネージャ の展開に展開します。

（注） LDAP ディレクトリ同期の設定方法については、*Cisco Unified Communications Manager* システム構成ガイドの「エンド ユーザの構成」の部分を参照してください。

手順

Step 1 Cisco Unified CM の管理で、**システム** > **LDAP** > **LDAPディレクトリ** を選択します。

Step 2 次のいずれかを実行します。

- [検索（Find）] をクリックし、既存の LDAP ディレクトリ同期を選択します。
- [新規追加（Add New）] をクリックして、新しい LDAP ディレクトリ同期を作成します。

Step 3 [機能グループテンプレート（Feature Group Template）] ドロップダウン リスト ボックスから、前のタスクで作成した機能グループ テンプレートを選択します。IM and Presence は、このテンプレートで無効にする必要があります。

Step 4 [LDAPディレクトリ（LDAP Directory）] ウィンドウで残りのフィールドを設定します。フィールドとその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。

Step 5 [保存（Save）] をクリックします。

Step 6 [完全同期を実施（Perform Full Sync）] をクリックします。
Cisco Unified Communications Manager は、データベースを LDAP ディレクトリと同期させ、更新された IM and Presence 設定を割り当てます。

次のタスク

中央クラスタへの連絡先リストのインポート（359 ページ）

一括管理を介した IM and Presence ユーザの有効化

ユーザをすでに中央クラスタに同期させており、それらのユーザが IM and Presence サービスに対して有効になっていない場合は、一括管理の [ユーザの更新(Administration's Update)] 機能を使用して、それらのユーザを IM and Presence サービスに対して有効にします。

（注） 一括管理の [ユーザのインポート(Administration's Import)] または [ユーザの挿入(Insert Users)] 機能を使用して、CSVファイルを介して新しいユーザをインポートすることもできます。手順は、*Cisco Unified Communications Manager* 一括管理ガイドを参照してください。インポートしたユーザ で、下記のオプションが選択されていることを確認します。

- [ホームクラスタ（Home Cluster）]
- [Unified CM IM and Presence のユーザを有効にする（Enable User for Unified CM IM and Presence）]

手順

Step 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）]から、**[一括管理（Bulk Administration）] > [ユーザ（Users）] > [ユーザの更新（Update Users）] > [クエリ（Query）]** の順に選択します。

Step 2 **フィルタ**で、**ホーム クラスタが有効になっている**を選択して、**検索(Find)**をクリックします。このウィンドウには、ここをホーム クラスタとするすべてのエンド ユーザが表示されます。

Step 3 [次へ（Next）] をクリックします。
ユーザ設定の更新 ウィンドウの一番左のチェックボックスで、この設定をこのクエリで編集するかどうかが表示されます。左側のチェック ボックスをチェックしないと、フィールドはクエリによって更新されません。右側のフィールドは、このフィールドの新しい設定を示しています。2 つのチェックボックスが表示されている場合は、左側のチェックボックスをオンにしてフィールドを更新し、右側のチェック ボックスには新しい設定を入力する必要があります。

Step 4 **サービス設定**で、以下の各フィールドの左側のチェックボックスをオンにして、これらのフィールドを更新することを示し、隣接するフィールドの設定を次のように編集します。

- **ホームクラスタ**: このクラスタをホームクラスタとして有効にするには、右側のチェックボックスをオンにします。

- **Unified CM IM and Presence でのユーザの有効化**：右のチェックボックスを確認します。この設定により、中央クラスタがこれらのユーザの IM and Presence サービスのプロバイダーとして有効となります。

Step 5 更新が必要な残りのフィールドをすべて入力します。フィールドとその設定を含むヘルプは、オンライン ヘルプを参照してください。

Step 6 **ジョブ情報**の下の**今すぐ実行(Run Immediately)**を選択します。

Step 7 [Submit] をクリックします。

中央クラスタへの連絡先リストのインポート

ユーザーを IM and Presence Central クラスタに移行した場合は、この手順を使用してユーザの連絡先リストを IM and Presence 中央クラスタにインポートすることができます。以下のいずれかのタイプの連絡先グループがインポート可能です。

- 連絡先リスト：このリストは、IM and Presence 連絡先で構成されます。
- 非プレゼンス連絡先リスト：このリストは、IMアドレスを持っていない連絡先で構成されます。

始める前に

古いクラスタ（テレフォニークラスタ）からエクスポートした連絡先リストの csv ファイルが必要となります。

手順

Step 1 IM and Presence セントラル クラスタ上の Cisco Unified CM IM and Presence 管理にログインします。

Step 2 テレフォニー クラスタからエクスポートした csv ファイルをアップロードします。

a) **一括管理(Bulk Administration)** > **ファイルをアップロード/ダウンロード(Upload/Download Files)** を選択します。
b) [新規追加（Add New）] をクリックします。
c) **ファイルの選択(Choose File)** をクリックして、インポートする csv ファイルを選択します。
d) **対象の選択** ドロップダウンで、インポートする連絡先リストの種類に応じて、以下のいずれかを選択します。**連絡先リスト** または **非プレゼンス連絡先リスト**。
e) **トランザクション タイプの選択**で、インポート ジョブを選択します。
f) **[保存（Save）]** をクリックします。

Step 3 Csv 情報を中央クラスタにインポートします。

a) Cisco Unified CM IM and Presence 管理で、以下のいずれかを実行します。
   - 連絡先リストのインポートの場合は、**一括管理(Bulk Administration)** > **連絡先リスト(Contact Lists)** > **連絡先リストの更新(Update Contact Lists)**を選択します。

- 非プレゼンス連絡先リストインポートの場合は、**一括管理(Bulk Administration)** > **非プレゼンス連絡先リスト(Non-presence Contact Lists)** > **非プレゼンス連絡先リストのインポート(Import Non-presence Contact Lists)**を選択します。

b) **ファイル名**ドロップダウンで、アップロードした csv ファイルを選択します。
c) **ジョブ情報**の下で、ジョブを実行したい時期に合わせて、**すぐに実行する** または **後で実行する** を選択します。
d) [送信（Submit）]をクリックします。**すぐに実行する** を選択した場合、連絡先リストはすぐにインポートされます。

（注） 。**後で実行する**を選択した場合、**一括管理** > **ジョブ スケジューラ** を開き、ジョブを選択して、実行する時間をスケジュールします。

Step 4 2 個目の csv ファイルをインポートする場合は、この手順を繰り返します。

次のタスク

Cisco Intercluster Sync Agentを起動する （360 ページ）

Cisco Intercluster Sync Agentを起動する

設定または移行が完了したら、IM and Presence 中央クラスタで **Cisco Intercluster Sync Agent** を開始します。クラスタ間ピアリングを使用している場合、このサービスが必要です。

手順

Step 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-ネットワークサービス（Control Center - Network Services）]** を選択します。

Step 2 **サーバ** ドロップダウンから 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。

Step 3 **IM and Presence サービス** の下の **Cisco Intercluster Sync Agent** を選択して、**起動(Start)**をクリックします。

次のタスク

中央クラスタのハイ アベイラビリティの有効化 （360 ページ）

中央クラスタのハイ アベイラビリティの有効化

設定またはユーザの移行が完了したら、IM and Presence 中央クラスタのプレゼンス冗長グループ（サブクラスタ）でハイ アベイラビリティを有効にします。

手順

Step 1 IM and Presence セントラル クラスタ上の Cisco Unified CM 管理インスタンスにログインします。

Step 2 **[System（システム）] > [Presence Redundancy Groups（プレゼンス冗長グループ）]** を選択します。

Step 3 **検索(Find)** をクリックして、既存のサブ クラスタを選択します。

Step 4 **ハイ アベイラビリティの有効化**のチェックボックスをチェックします。

Step 5 **[保存（Save）]** をクリックします。

Step 6 IM and Presence 中央クラスタの各クラスタに対してこの手順を繰り返します。

移行クラスタの残りのピアを削除する

移行クラスタ (現在はテレフォニークラスタ) とその他の IM and Presence サービスピアクラスタ間のクラスタ間ピア関係を削除します。

（注） クラスタ間接続の削除は、メッシュ全体での Cisco XCP ルータの再起動の可用性に応じて、後の日付に延期することができます。テレフォニークラスタと任意の数のピアクラスタの間に既存のクラスタ間接続がある限り、現在Cisco XCPルータサービスを実行している場合は、テレフォニークラスタで**実行**状態のままにする必要があります。

手順

Step 1 移行クラスタの IM and Presence データベース パブリッシャ ノードにログインします。

Step 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。

Step 3 **検索(Find)** をクリックしてピアクラスタを選択します。

Step 4 [削除（Delete）] をクリックします。

Step 5 **Cisco XCP ルータ**を再起動します：

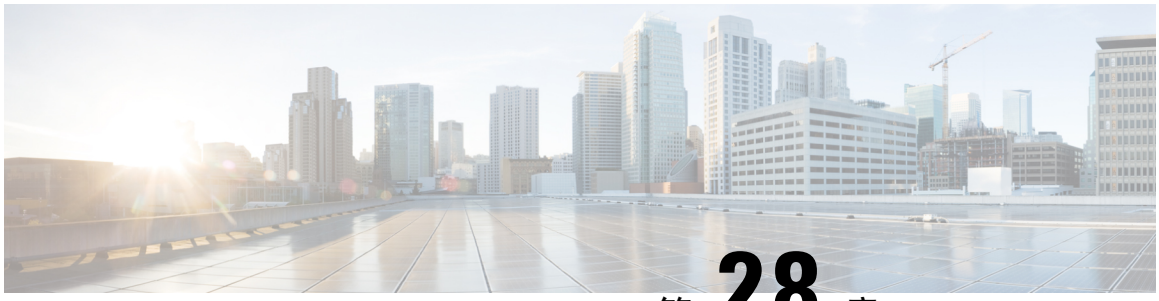
a) Unified IM and Presence Serviceability にログインして、**ツール(Tools)** > **コントロール センター - ネットワーク サービス(Control Center - Network Services)**を選択します。

b) **サーバ** リストから、データベース パブリッシャ ノードを選択して、**移動(Go)**をクリックします。

c) [IM and Presenceサービス（IM and Presence Services）] の下で、[Cisco XCPルータ（Cisco XCP Router）] を選択し、[リスタート(Restart)] をクリックします

Step 6 IM and Presence サービス ピア クラスタでこれらの手順を繰り返します。

（注） 移行クラスタに複数のクラスタへのクラスタ間ピア接続がある場合は、クラスタ間ネットワークに残っている各ピアクラスタに対してこの手順を繰り返す必要があります。つまり、移行するクラスタでは、破損しているピアクラスタ接続があるため、**Cisco XCP ルータ**が再起動するサイクルは多数あります。



第 28 章

ユーザの移行

ユーザ移行の概要

ここでは、IM and Presence Service クラスタ間でユーザを移行する方法について説明します。

移行の要件

- 現在のクラスタおよび移動先クラスタの両方の完全バックアップを行います。詳細については、バックアップ タスク フロー （400 ページ）を参照してください。
- 移行するユーザに現在の（移行前）ホーム クラスタ上の Cisco Unified Presence または Cisco Jabber のライセンスが供与されていることを確認します。これらのユーザーが移行元クラスタ以外のクラスタでライセンスされている場合は、移行作業を進める前に完全にライセンスを解除しておく必要があります。

ユーザ移行タスク フロー

IM and Presence ユーザを新しいクラスタに移行するには、これらのタスクを完了します。

手順

	コマンドまたはアクション	目的
Step 1	古いエントリを削除する （365 ページ）	ユーザを移行する前に、すべての古い rosters、グループエントリ、および非プレゼンス契約レコードを削除します。

	コマンドまたはアクション	目的
Step 2	移動の必須サービスの起動（367ページ）	移行する前に、以下のサービスが実行されていることを確認します。 • Cisco AXL Web Service • Cisco Sync Agent • Cisco Intercluster Sync Agent
Step 3	クラスタ間同期エラーの確認（366ページ）	トラブル シューティングを実行し、Intercluster Sync Agent に問題がないことを確認します。
Step 4	移行の標準プレゼンスの設定（366ページ）	ユーザを移行する前に、以下の標準のプレゼンス設定を構成します。
Step 5	ユーザ連絡先リストのエクスポート（367ページ）	この手順を実行して、移行中のユーザーの連絡先リストを現在のクラスタからエクスポートします。
Step 6	以下のいずれかのミニ タスク フローを完了して、ユーザを新しいクラスタに移動します。 • LDAP 経由でのユーザの移行（368ページ） • 新しいクラスタへのユーザの手動での移動（370ページ） • 一括管理経由のユーザ移行（373ページ）	ユーザを新しいクラスタに移動します。LDAPを使用して、新しいクラスタにユーザをプロビジョニングすること、ユーザを手動で移動すること、あるいは一括管理を使用して、ユーザを新しいクラスタに移行することが可能です。
Step 7	ホーム クラスタでの連絡先リストのインポート（378ページ）	ユーザを新しいクラスタに移行したら、連絡先リストをインポートして、移行したユーザの連絡先データを復元します。
Step 8	元のクラスタでのユーザの更新（379ページ）	新しいクラスタですべてが正常に動作していることを確認するまで、古いクラスタからユーザーを削除しないでおくこともできます。一括管理のユーザの更新機能を使用するこの手順を使用して、古いクラスタから IM and Presence 機能を削除します。

古いエントリを削除する

ユーザを移行する前に、古い rosters、グループエントリ、および非プレゼンス連絡先レコードを削除します。これは、ユーザがプレゼンスを無効にしたパブリッシャ IM&P ノードで実行されます。

（注） 必要に応じて、2000のバッチでこれらの手順を繰り返します。CLI を介して大量の古いエントリを削除するのに時間がかかっている場合は、TAC ケースをオープンして、ルートアクセスが必要なこのセクションの最後にある古い名簿スクリプトを活用します。

手順

Step 1 CLI セッションを開始します。CLI セッションを開始する方法の詳細については、『*Cisco Unified Communications* ソリューション コマンドライン インターフェイス リファレンス ガイド』の「CLI セッションの開始」の項を参照してください。

Step 2 古い名簿エントリを確認して削除します。これを行うには、次のクエリを実行します。

a) 古い名簿のエントリがないかどうかを確認します。

```
run sql select count(*) from rosters where user_id in (select xcp_user_id from enduser
where primarynodeid is NULL)
```

b) 古い名簿のエントリを削除します。

```
run sql delete from rosters where pkid in (select * from (select first 2000 pkid from
rosters where user_id in (select xcp_user_id from enduser where primarynodeid is NULL)))
```

Step 3 古いグループレコードを確認して削除します。これを行うには、次のクエリを実行します。

a) 古いグループレコードがないかどうかを確認します。

```
run sql select count(*) from groups where user_id in (select xcp_user_id from enduser
where primarynodeid is NULL)
```

b) 古いグループレコードを削除します。

```
run sql delete from groups where pkid in (select * from (select first 2000 pkid from
groups where user_id in (select xcp_user_id from enduser where primarynodeid is NULL)))
```

Step 4 古い非連絡先レコードを確認して (順番に) 削除します。これを行うには、次のクエリを実行します。

a) 古い非連絡先レコード (順番) を確認します。

```
run sql select count(*) from nonpresencecontacts where fkenduser in (select pkid from
enduser where primarynodeid is null)
```

b) 古い非連絡先レコードを次の順序で削除します。

```
run sql delete from nonpresencecontacts where pkid in (select * from (select first 2000
 pkid from nonpresencecontacts where fkenduser in (select pkid from enduser where
primarynodeid is null)))
```

c) ルートアクセス権がある場合は、次のクエリを使用します。

```
run sql delete from epascontactaddinfo where pkid in (select * from (select first 2000
pkid from epascontactaddinfo where pkid not in (select fkepascontactaddinfo from
nonpresencecontacts)))
```

移行の標準プレゼンスの設定

ユーザを移行する前に、以下のプレゼンス設定を構成します。

手順

Step 1 Cisco Unified CM IM and Presence 管理で、**プレゼンス** > **設定** > **標準設定**を選択します。

Step 2 **確認プロンプトなしで、ユーザが他のユーザのプレゼンスステータスを表示できるようにする**l チェックボックスをオンにします。

Step 3 **連絡先リストの最大サイズ（ユーザ毎）** で、**制限なし** チェック ボックスをオンにします。

Step 4 **ウォッチャの最大数（ユーザ毎）** 設定では、**無制限** チェックボックスをオンにします。

Step 5 [保存（Save）] をクリックします。

次のタスク

クラスタ間同期エラーの確認 （366 ページ）

クラスタ間同期エラーの確認

移行する前に、クラスタ間の同期エラーが発生していないことを確認します。

手順

Step 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（System Troubleshooter）]** を選択します。

Step 2 クラスタ間の同期エラーが発生していないことを確認します。エラーがある場合は、修正を行ってから続行します。

次のタスク

移動の必須サービスの起動 （367 ページ）

移動の必須サービスの起動

Cisco Unified IM and Presence Serviceability において、以下の移行の重要なサービスが実行されていることを確認します。

- Cisco AXL Web Service
- Cisco Sync Agent
- Cisco Intercluster Sync Agent

手順

Step 1 Cisco Unified IM and Presence Serviceabilityから、**ツール** > **コントロールセンター - 機能サービス** を選択します。

Step 2 **サーバ** ドロップダウンから、使用する IM and Presence クラスタ ノードを選択し、**移動**をクリックします。

Step 3 **データベースおよび管理サービス**の下の **Cisco AXL Web Service** が起動していることを確認します。サービスが、実行中でない場合（デフォルト設定が実行中でない場合）、そのサービスを選択して、**起動**をクリックします。

Step 4 **[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）]** を選択します。

Step 5 **サーバ** ドロップダウンから、使用する IM and Presence クラスタ ノードを選択し、**移動**をクリックします。

Step 6 **IM and Presence Services**の下の**Cisco Sync Agent** および **Cisco クラスタ間 Sync Agent** サービスの両方が実行中であることを確認します。実行されていない場合は、**起動**させます。

次のタスク

ユーザ連絡先リストのエクスポート （367 ページ）

ユーザ連絡先リストのエクスポート

この手順を実行して、移行中のユーザーの連絡先リストを現在のクラスタからエクスポートします。

手順

Step 1 現在のホーム クラスタから移行ユーザの連絡先リストをエクスポートします。

a) **Cisco Unified CM IM and Presence 管理**で、**一括管理** > **連絡先リスト** > **エクスポート**を選択します。

b) **クラスタ内のすべての未割当てユーザ** を選択して、**検索**をクリックします。

c) 結果を確認し、必要に応じて **[AND/OR（および/また）]** フィルタを使用して検索結果をフィルタリングします。
d) リストが完了したら、**次へ** をクリックします。
e) エクスポートされた連絡先リスト データのファイル名を選択します。
f) 任意でジョブの説明を更新します。
g) **[今すぐ実行（Run Now）]** をクリックするか、ジョブを後で実行するようにスケジュールします。

Step 2 連絡先リストのエクスポート ジョブのステータスをモニタします。

a) **Cisco Unified CM IM and Presence 管理**で、**一括管理** > **ジョブ スケジューラ**を選択します。
b) **検索** をクリックして、すべての BAT ジョブをリストします。
c) 連絡先リストのエクスポート ジョブを検索し、それが完了と報告された場合はジョブを選択します。
d) [CSV ファイル名（CSV File Name）] リンクを選択して、連絡先リストのエクスポート ファイルの内容を表示します。ファイル名にタイム スタンプが追加されます。
e) **[Job Results（ジョブの結果）]** セクションから、アップロードされた内容の要約を表示するログ ファイルを選択します。ログ ファイルには、ジョブの開始時刻、終了時刻、および結果の概要が含まれます。

Step 3 後でユーザの移行が完了したときに使用できるように、連絡先リストのエクスポート ファイルをダウンロードし、保存します。

a) **Cisco Unified CM IM and Presence 管理**で、**一括管理** > **ファイルのアップロード/ダウンロード**を選択します。
b) [検索（Find）] をクリックします。
c) 連絡先リストのエクスポート ファイルを選択し、**[選択項目のダウンロード（Download Selected）]** を選択します。
d) 後の手順でアップロードできるように CSV ファイルをローカルに保存します。

次のタスク

以下のタスク フローのいずれかに移動して、新しいクラスタ内のユーザを割り当てます。

- LDAP 経由でのユーザの移行 （368 ページ）
- 新しいクラスタへのユーザの手動での移動 （370 ページ）

LDAP 経由でのユーザの移行

ユーザが LDAP ディレクトリと同期されていて、新しいクラスタに移行する場合は、以下のタスクを実行します。

（注） LDAPディレクトリの設定を新しいクラスタに追加する必要があります。これには、すべてのサービス プロファイル、ユーザ プロファイル、および機能グループ テンプレートが含まれます。機能グループテンプレートの設定で、**Unified CM IM and Presence のユーザを有効にする** チェックボックスがオンになっていることを確認します。

手順

	コマンドまたはアクション	目的
Step 1	外部LDAPディレクトリの更新（369ページ）	クラスタ毎に別々のLDAP構造を使用し、ユーザが自身のホーム クラスタにのみ同期される展開の場合は、外部 LDAP ディレクトリを更新する必要があります。
Step 2	新しいクラスタでの LDAP の設定 （370ページ）	Cisco Unified Communications Manager で LDAPが有効である場合は、新しいクラスタを更新された LDAP ディレクトリと同期させて、ユーザを新しいクラスタにインポートします。

次のタスク

ホーム クラスタでの連絡先リストのインポート （378 ページ）

外部 LDAP ディレクトリの更新

クラスタ毎に別々の LDAP 構造を使用し、ユーザが自身のホーム クラスタにのみ同期される展開の場合は、外部 LDAP ディレクトリを更新する必要があります。

（注） 展開でフラットな LDAP 構造を使用する場合、つまり、すべてのユーザがすべての Cisco Unified Communications Manager および IM and Presence サービス クラスタに同期され、ユーザが 1 つのクラスタにのみライセンスされている場合は、ユーザを移動する必要はありません。

（注） 移行元・移行先のクラスタで LDAP ディレクトリ同期の設定内容に応じて、外部 LDAP ディレクトリ内でユーザを移動すると、次回の同期が実行される際、それらのユーザが自動的に新しい IM and Presence サービス クラスタに移行される場合があります。

手順

Step 1 外部 LDAP ディレクトリ内のユーザを更新します。

Step 2 ユーザの移動後、古い LDAP のクラスタから LDAP エントリを削除します。

次のタスク

新しいクラスタでの LDAP の設定 （370 ページ）

新しいクラスタでの LDAP の設定

始める前に

新しいクラスタで LDAP ディレクトリをプロビジョニングします。LDAPディレクトリ同期にユニバーサル回線テンプレート、デバイステンプレート、および機能グループテンプレートが含まれている場合は、新しいクラスタでこれらのテンプレートを設定する必要があります。機能グループ テンプレートで、以下のオプションがオンになっていることを確認します。

- Home Cluster
- Unified CM IM and Presence のユーザの有効化

LDAP ディレクトリ同期の設定方法については、*Cisco Unified Communications Manager* システム設定ガイドの「エンド ユーザの構成」の部分を参照してください。

手順

Step 1 Cisco Unified CM の管理で、**[System（システム）] > [LDAP（LADP）] > [LDAP Directory（LDAP ディレクトリ）]** を選択します。

Step 2 **検索** をクリックして、設定した LDAP ディレクトリを選択します。

Step 3 [完全同期を今すぐ実施（Perform Full Sync Now）] をクリックします。

次のタスク

ホーム クラスタでの連絡先リストのインポート （378 ページ）

新しいクラスタへのユーザの手動での移動

ユーザを新しいクラスタに手動で移動するには、以下のタスクを実行します。

（注） ユーザ数が多い場合は、Cisco Unified Communications Manager の一括管理ツールを使用して、csv ファイル経由で多数のユーザを更新します。詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。

手順

	コマンドまたはアクション	目的
Step 1	ユーザの IM and Presence の手動での無効化 （371 ページ）	現在のホーム クラスタで IM and Presence Service と Cisco Jabber へ移行するユーザを無効にします。
Step 2	ユーザの手動インポート （372 ページ）	新しいクラスタに LDAP 同期が設定されていない場合は、ユーザを新しい Cisco Unified Communications Manager クラスタに手動でプロビジョニングします。
Step 3	新しいクラスタの IM and Presence サービスのユーザの有効化 （372 ページ）	新しいホーム クラスタでユーザが同期されている場合、または手動でプロビジョニングされている場合は、手動で IM and Presence サービスおよび Cisco Jabber のユーザを有効にする必要があります。

次のタスク

ホーム クラスタでの連絡先リストのインポート （378 ページ）

ユーザの IM and Presence の手動での無効化

次の手順では、現在のホーム クラスタの IM and Presence Service および Cisco Jabber の移行ユーザを無効にする方法について説明します。

（注） 一度に移行するユーザ数が多い場合は、Cisco Unified Communications Managerの一括管理ツールを使用することを推奨します。詳細は、 *Cisco Unified Communications Manager* 一括管理ガイドを参照してください。

始める前に

ユーザ連絡先リストのエクスポート （367 ページ）

手順

Step 1 **Cisco Unified CM 管理**で、> **ユーザ管理** > **エンド ユーザ**を選択します。

Step 2 フィルタを使用して、IM and Presence Service を無効にするユーザを検索します。

Step 3 [エンド ユーザの設定（End User Configuration）] 画面で、**[Unified CM IM and Presence にユーザを有効にします（Enable User for Unified CM IM and Presence）]** チェックボックスをオフにします。

Step 4 [保存（Save）] をクリックします。

次のタスク

ユーザの手動インポート （372 ページ）

ユーザの手動インポート

新しいクラスタに LDAP 同期が設定されていない場合は、ユーザを新しい Cisco Unified Communications Manager クラスタに手動でインポートします。

詳細については、「ユーザ設定値の設定 （79 ページ）」を参照してください。

次のタスク

新しいクラスタの IM and Presence サービスのユーザの有効化 （372 ページ）

新しいクラスタの IM and Presence サービスのユーザの有効化

新しいホーム クラスタでユーザが同期されている場合、または手動でプロビジョニングされている場合は、手動で IM and Presence サービスおよび Cisco Jabber のユーザを有効にする必要があります。

手順

Step 1 **Cisco Unified CM 管理**で、**ユーザ管理** > **エンド ユーザ**を選択します。

Step 2 フィルタを使用して、IM and Presence サービスを有効にするユーザを検索します。

Step 3 [エンド ユーザの設定（End User Configuration）] 画面で、[Unified CM IM およびプレゼンスにユーザを有効にします（Enable User for Unified CM IM and Presence）] をオンにします。

Step 4 [保存（Save）] をクリックします。

Step 5 電話機および CSF の Cisco Unified Communications Manager のユーザをプロビジョニングします。詳細については、『*Upgrade Guide for the Cisco Unified Communications Manager*』を参照してください。

次のタスク

ホーム クラスタでの連絡先リストのインポート（378 ページ）

一括管理経由のユーザ移行

一括管理ツールを使用して、ユーザを新しいクラスタに移動します（たとえば、クラスタ 1 からクラスタ 2 への移行）。

始める前に

Cisco一括プロビジョニング サービスが、両方のクラスタで実行されている必要があります。

（注） IM and Presence クラスタ内の送信元から宛先へ移動するユーザの数が100未満の場合は、Cisco Intercluster Sync Agent サービスを開始または停止しないでください。

任意の送信元/宛先クラスタから 100 ~ 1000 ユーザを移動する場合は、ソースクラスタと宛先クラスタの両方で Intercluster Sync Agent サービスを停止して、次の手順を実行します。

移動するユーザの数が1000を超えている場合、たとえば、16 k のユーザを移動する必要がある場合は、次の手順に従って 8 k のユーザを最初に移動し、ユーザを 1 k のユーザのチャンクに移動しながら Intercluster Sync Agent サービスを停止します。後で、1 k のユーザのチャンクでバランスが取れたシリアルシーケンスで次の8K を移動します。

ユーザがソースから移動されている IM and Presence クラスタで、次のようにします。

ステップ 1IM and Presence パブリッシャのプレゼンス冗長グループ (PRG) ペアがクラスタ間同期エージェントサービスを停止する、関連付けられたサブスクライバノード上。

ステップ 2パブリッシャ IM and Presence プレゼンス冗長グループペアのクラスタ間同期エージェントサービスを停止するパブリッシャノード上。

ユーザが接続先から移動されている IM and Presence クラスタで、次のようにします。

ステップ 3パブリッシャプレゼンス冗長グループペアのクラスタ間同期エージェントサービスを停止するセカンダリノード上。

ステップ 4パブリッシャプレゼンス冗長グループペアのクラスタ間同期エージェントサービスを停止するパブリッシャノード上。

（注） クラスタ間同期エージェントサービスを停止する必要がある他のクラスタノードはありません。

ステップ 5 Perform 一括管理によるユーザの移行に記載されている手順を実行します。

ステップ 6IM and Presence パブリッシャおよびサブスクライバノードのクラスタ間同期エージェントサービスを、宛先クラスタとソースクラスタの両方で開始します。

ステップ 7他のすべてのクラスタが宛先クラスタとの同期を完了するまでに最大30分かかることがあります。

手順

	コマンドまたはアクション	目的
Step 1	CSV ファイルへのユーザ エクスポート（374 ページ）	移行元のクラスタ（クラスタ 1）で、移行するユーザを CSV ファイルにエクスポートします。
Step 2	CSV エクスポート ファイルのダウンロード（375 ページ）	CSV エクスポート ファイルをダウンロードします。
Step 3	新しいクラスタへのCSVエクスポートファイルのアップロード（375 ページ）	CSV ファイルを移行先クラスタ（クラスタ 2）にアップロードします。
Step 4	ユーザテンプレートの設定（376ページ）	移行先クラスタで、ユーザ設定を使用して、ユーザ テンプレートを設定します。
Step 5	新しいクラスタへのユーザの移行（376 ページ）	CSV ファイルからユーザをインポートするには、一括管理の [ユーザの挿入] メニューを使用します。
Step 6	一括管理によるユーザー移行の確認（377 ページ）	一括管理によるユーザの移行を確認します。

CSV ファイルへのユーザ エクスポート

移行元のクラスタで、一括管理ツールを使用して、移行するユーザを CSV ファイルにエクスポートします。

注意：ジョブの実行後は、ジョブ スケジューラに移動して、ジョブのステータスを確認し、ファイルが作成されたことを確認することができます。[後で実行する] を選択した場合、ジョブ スケジューラを使用してジョブの実行時間を設定することができます。

手順

Step 1 Cisco Unified CM Administration から、**[一括管理（Bulk Administration）] > [ユーザ（Users）] > [ユーザのエクスポート（Export Users）]** の順に選択します。

Step 2 **フィルタ** ツールを使用して、移行するユーザを検索して選択し、**検索**をクリックします。

Step 3 [次へ（Next）] をクリックします。

Step 4 ファイルの**ファイル名**を入力します。
このツールは、ファイルの末尾に `.txt`拡張子を追加します。たとえば、`<csvfilename>.txt` となります。

Step 5 **ファイル形式**のドロップダウンから、エクスポート ファイルの形式を選択します。

Step 6 ジョブをすぐに実行する場合、**今すぐ実行** をクリックして、**送信**をクリックします。

次のタスク

ジョブの実行後は、**ジョブ スケジューラ**に移動して、ジョブのステータスを確認し、ファイルが作成されたことを確認することができます。**後で実行する**を選択した場合、ジョブ スケジューラを使用してジョブの実行時間を設定することができます。

ファイルが作成されたことを確認したら、CSV エクスポート ファイルのダウンロード（375 ページ）。

CSV エクスポート ファイルのダウンロード

エクスポート ファイルが作成されたことを確認した後、ファイルをダウンロードします。

手順

Step 1 Cisco Unified CM Administration から、**[一括管理（Bulk Administration）]>[ファイルのアップロード/ダウンロード（Upload/Download Files）]** を選択します。

Step 2 [検索（Find）] をクリックします。

Step 3 作成されたファイルを選択して、**選択したファイルをダウンロードする**をクリックします。

Step 4 ファイルをダウンロードします。

次のタスク

新しいクラスタへのCSV エクスポート ファイルのアップロード（375 ページ）

新しいクラスタへのCSV エクスポート ファイルのアップロード

移動先クラスタ（クラスタ 2）で、クラスタ 1 からエクスポートした CSV ファイルをアップロードします。

手順

Step 1 Cisco Unified CM Administration から、**[一括管理（Bulk Administration）]>[ファイルのアップロード/ダウンロード（Upload/Download Files）]** を選択します。

Step 2 [新規追加（Add New）] をクリックします。

Step 3 [Choose File] をクリックします。別のシステムからエクスポート ファイルを参照して選択します。

Step 4 **対象** ドロップダウンから、ファイル内容をインポートするために使用する一括管理メニューを選択します。たとえば、**ユーザ**あるいは**電話機、およびユーザ**を選択します。

Step 5 **トランザクションタイプ**ドロップダウンから、ファイルの内容をインポートするために使用するサブ メニューを選択します。たとえば、**ユーザの挿入** または**電話/ユーザの挿入**を行います。

Step 6 [保存（Save）] をクリックします。

次のタスク

ユーザ テンプレートの設定 （376 ページ）

ユーザ テンプレートの設定

移動先クラスタで、インポートしたユーザに適用する設定で、ユーザ テンプレートを設定します。

手順

Step 1 Cisco Unified CM 管理から、**一括管理** > **ユーザ** > **ユーザのエクスポート**を選択します。

Step 2 次のいずれかを実行します。

- **検索** をクリックして、既存のテンプレートを選択します。
- [新規追加（Add New）] をクリックして新しいテンプレートを作成します。

Step 3 インポートされたユーザに適用するユーザ設定を構成します。たとえば、以下のフィールドがオンになっていることを確認します。

- **[ホームクラスタ（Home Cluster）]**
- **[Unified CM IM and Presence のユーザを有効にする（Enable User for Unified CM IM and Presence）]**

Step 4 Microsoft Outlook を使用してカレンダーを統合するためにユーザを有効にする場合は、**プレゼンス に会議情報を含める**チェックボックスをオンにします。

Step 5 残りのフィールドを設定します。

Step 6 [保存（Save）] をクリックします。

次のタスク

新しいクラスタへのユーザの移行 （376 ページ）

新しいクラスタへのユーザの移行

一括管理の [ユーザの挿入] メニューを使用して、エクスポートしたユーザを新しいクラスタにインポートします。

手順

Step 1 Cisco Unified CM 管理から、**一括管理** > **ユーザ** > **ユーザのインポート**を選択します。
Step 2 **ファイル名**から、他のシステムからエクスポートされたファイルを選択します。
Step 3 **ユーザテンプレート名**から、先ほど作成したユーザテンプレートを選択します。
Step 4 **ユーザのエクスポートで作成されたファイル** で作成されたファイルを確認します。
Step 5 **今すぐ実行**をクリックして、**送信**をクリックします。

次のタスク

ホーム クラスタでの連絡先リストのインポート （378 ページ）

一括管理によるユーザー移行の確認

一括管理を使用してユーザを移行した後、ソースクラスタと宛先クラスタでCisco Intercluster Sync Agentサービスを開始した後、送信元と宛先のクラスタとは別のクラスタが、ユーザの移動によって通知を受信したことを確認する必要があります。発生しました。

他のすべてのクラスタが宛先クラスタとの同期を完了するまでに最大30分かかることがあります。待機している間は、変更 (送信元または宛先) の一部ではない並行してサンプル (5) IMP パブリッシャへのターミナルセッションを開いて、CiscoSyslogs をモニタすることができます。

手順

Step 1 次のコマンドを実行して、一括管理によるユーザの移行後にサンプル IMP パブリッシャノードがすでに同期を完了しているかどうかを確認し、送信元および宛先クラスタでCisco Intercluster Sync Agentサービスを開始します。この時点でタイムスタンプに通知します。次の構文の例では、宛先クラスタ名は dst 名です。これを宛先クラスタ名に置き換えます。

```
admin:file search activelog syslog/CiscoSyslog ".*InterClusterSyncAgentStatus:.*dst-name.*"
```

Step 2 ICSA ステータスのタイムスタンプが記録されたタイムスタンプよりも新しいものではない場合は、同期が正常に完了するまで、最大で30分間次のコマンドを使用します。

```
admin:file tail activelog syslog/CiscoSyslog regexp
".*InterClusterSyncAgentStatus:.*dst-name.*"
```

選択したサンプルクラスタ/ノードで ICSA failed sync status アラームが表示された場合は、同期ステータスアラームが正常に完了するまで5-10 分待ちます。ICSA は5分ごとに再試行されます。同期が正常に完了していないか、同期が一貫していない場合は、TAC ケースをオープンしてください。

この時点で、5つのリモートサンプルクラスタを確認しました。これは、一括管理によるユーザの移行後、および送信元クラスタと宛先クラスタでCisco Intercluster Sync Agent サービスを開始した

後に、現在の時刻がタイムスタンプよりも30分後に記録された場合です。これで、次の移動プロセスに進むことができます。その他の移動がない場合は、終了します。

ホーム クラスタでの連絡先リストのインポート

ユーザを新しいクラスタに移行したら、連絡先リストをインポートして、移行したユーザの連絡先データを復元します。

手順

Step 1 前にエクスポートされた連絡先リストの CSV ファイルをアップロードします。

a) **Cisco Unified CM IM and Presence 管理**で、**一括管理** > **ファイルのアップロード/ダウンロード**を選択します。
b) **[新規追加]** をクリックします。
c) 連絡先リストの CSV ファイルを選択するには、**[参照（Browse）]** をクリックします。
d) ターゲットとして **[連絡先リスト（Contact Lists）]** を選択します。
e) トランザクション タイプとして [ユーザの連絡先のインポート - カスタム ファイル（Import Users' Contacts – Custom File）] を選択します。
f) 必要に応じて **[ファイルが存在する場合は上書きする（Overwrite File if it exists）]** をオンにします。
g) **[Save（保存）]** を選択してファイルをアップロードします。
h) **[Save（保存）]** を選択してファイルをアップロードします。

Step 2 連絡先リスト ジョブのインポートを実行します。

a) **Cisco Unified CM IM and Presence 管理**で、**一括管理** > **連絡先リスト** > **更新**を選択します。
b) ステップ 1 でアップロードした CSV ファイルを選択します。
c) 任意でジョブの説明を更新します。
d) ジョブを今すぐ実行するには、**[今すぐ実行（Run Immediately）]** をクリックします。後で更新をスケジュールするには、**[後で実行（Run Later）]** を選択します。
e) [送信（Submit）] をクリックします。

Step 3 連絡先リストのインポート ステータス監視

a) **Cisco Unified CM IM and Presence 管理**で、**一括管理** > **連絡先リスト** > **ジョブ スケジューラ**を選択します。
b) **[検索（Find）]** をクリックして、すべての BAT ジョブをリストします。
c) ステータスが完了と報告されたら、連絡先リストのインポート ジョブのジョブ ID を選択します。
d) 連絡先リスト ファイルの内容を表示するには、**[CSV ファイル名（CSV File Name）]** にリストされているファイルを選択します。
e) **[ログ ファイル名（Log File Name）]** リンクをクリックし、ログを開きます。

ジョブの開始時刻と終了時刻が表示され、結果の要約も表示されます。

元のクラスタでのユーザの更新

新しいクラスタですべてが正常に動作していることを確認するまで、古いクラスタからユーザーを削除しないでおくこともできます。一括管理のユーザの更新機能を使用するこの手順を使用して、古いクラスタから IM and Presence 機能を削除します。

手順

Step 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）]から、**[一括管理（Bulk Administration）] > [ユーザ（Users）] > [ユーザの更新（Update Users）] > [クエリ（Query）]** の順に選択します。

Step 2 フィルタ ツールを使用して、移行ユーザを検索します。たとえば、以下条件を満たすユーザのすべてを検索することができます。**IM and Presence が有効になっているか**。

Step 3 [Next] をクリックします。

Step 4 以下の 2 つのフィールドのそれぞれについて、一番左のチェック ボックスをオンにして、隣の右側のチェック ボックスはオフのままにします。左側のボックスは、フィールドを更新することを示し、右側のボックスには新しい設定 (オフ) が示されています。

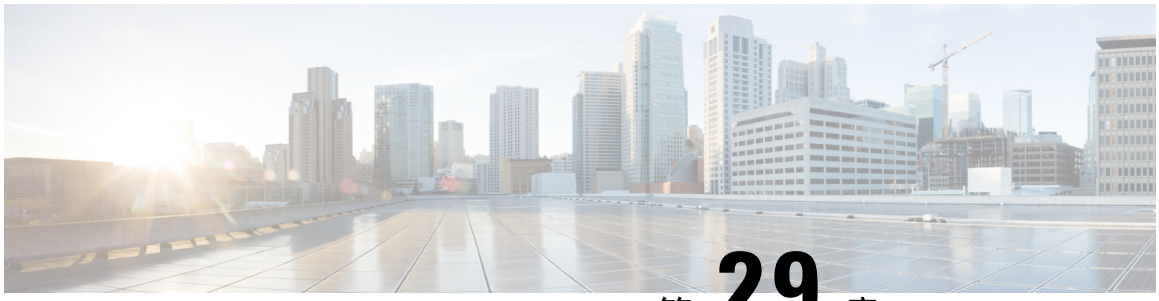
- **[ホームクラスタ（Home Cluster）]**
- **[Unified CM IM and Presence のユーザを有効にする（Enable User for Unified CM IM and Presence）]**

Step 5 **ジョブ情報**の下の**今すぐ実行(Run Immediately)**を選択します。

Step 6 [Submit] をクリックします。

次のタスク

移行が正常に実行されたこと、すべてのユーザが新しいクラスタで適切に設定されていることの確認ができたら、元のクラスタ内の移行したユーザを削除することができます。



第 29 章

ロケール管理

ロケール管理の概要

複数の言語をサポートする Cisco Unified Communications Manager と IM and Presence サービスを設定できます。インストール可能なサポート言語の数に制限はありません。

www.cisco.com には、ロケール固有のバージョンの Cisco Unified Communications Manager のロケール インストーラと IM and Presence サービスのロケール インストーラが用意されています。このロケール インストーラはシステム管理者がインストールします。このインストーラを使用すると、ユーザがサポートされているインターフェイスを使用するときに、選択した翻訳済みテキストまたはトーン（使用可能な場合）を表示または受信できます。

Cisco Unified Communications Manager または IM and Presence Service をアップグレードした後で、すべてのロケールを再インストールする必要があります。Cisco Unified Communications Manager ノードまたは IM and Presence Service ノードの major.minor バージョン番号と一致する、最新バージョンのロケールをインストールしてください。

クラスタの各ノードに Cisco Unified Communications Manager をインストールし、データベースをセットアップしてから、ロケールをインストールします。IM and Presence Service ノードで特定のロケールをインストールする場合は、最初に Cisco Unified Communications Manager のクラスタで同じ国の Cisco Unified Communications Manager のロケール ファイルをインストールする必要があります。

ソフトウェアのアップグレードが完了した後に、Cisco Unified Communications Manager のノードと IM and Presence サービス ノードでロケールをインストールするには、次の項の情報を使用します。

ユーザ ロケール

ユーザ ロケール ファイルは、特定の言語と国に関する言語情報が含まれます。ユーザ ロケール ファイルは、ユーザが選択したロケールの電話機表示用の翻訳済みテキストとボイス プロンプト（使用可能な場合）、ユーザアプリケーション、およびWebページを提供します。これらのファイル名の表記は、次のとおりです。

- cm-locale-language-country-version.cop（Cisco Unified Communications Manager）
- ps-locale-language_country-version.cop（IM and Presence Service）

システムでユーザ ロケールのみが必要な場合は、CUCM ロケールをインストールした後でそれをインストールします。

ネットワーク ロケール

ネットワーク ロケール ファイルは、電話トーン、Annunciator、ゲートウェイ トーンなど、さまざまなネットワーク項目の国固有のファイルを提供します。複合ネットワーク ロケール ファイル名の表記は、次のとおりです。

- cm-locale-combinednetworklocale-version.cop（Cisco Unified Communications Manager）

1 つのロケール インストーラに複数のネットワーク ロケールが組み合されている場合があります。

（注） シスコ認定の顧客が提供するサーバ上の Cisco Unified Communications Manager および IM and Presence Service は、複数のロケールをサポートします。複数のロケール インストーラをインストールすることにより、ユーザは複数のロケールから選択できるようになります。

ロケール ファイルは、ソフトウェア アップグレードをインストールする場合と同じプロセスを使用して、ローカル ソースまたはリモート ソースからインストールできます。クラスタの各ノードに、複数のロケール ファイルをインストールできます。クラスタ内のすべてのノードをリブートしないと、変更は有効になりません。クラスタ内のすべてのノードですべてのロケールのインストールが終了するまで、ノードをリブートしないように強くお勧めします。通常の業務時間後にノードをリブートして、コール処理の中断を最小限にとどめてください。

ロケール要件の管理

ロケールのインストールに関する考慮事項

- ロケールをインストールする前に、すべての Cisco Unified Communications Manager および IM and Presence Serviceのクラスタ ノードをインストールして、データベースを設定します。

- IM and Presence Service ノードで特定のロケールをインストールする場合は、最初に Cisco Unified Communications Manager のクラスタで同じ国の Cisco Unified Communications Manager のロケール ファイルをインストールする必要があります。
- クラスタの各ノードに、複数のロケール ファイルをインストールできます。新しいロケールをアクティブにするには、インストール後にクラスタの各ノードを再起動する必要があります。
- ロケールファイルは、ソフトウェアアップグレードをインストールする場合と同じプロセスを使用して、ローカル ソースまたはリモート ソースからインストールできます。ローカル ソースまたはリモート ソースからのアップグレードの詳細は、*Cisco Unified Communications Manager* アップグレード ガイド を参照してください。

IM and Presence Service へのロケール インストーラのインストール

- IM and Presence Service 用のロケールをインストールする前に、Cisco Unified Communications Manager にロケール インストーラをインストールします。英語以外のロケールを使用する場合は、Cisco Unified Communications Manager と IM and Presence Service の両方に適切な言語インストーラをインストールする必要があります。
- IM and Presence Service クラスタに複数のノードがある場合は、ロケール インストーラがクラスタ内のすべてのノードにインストールされていることを確認します（サブスクライバ ノードの前に IM and Presence データベース パブリッシャ ノードにインストールします）。
- 適切なすべてのロケールインストーラが両方のシステムにロードされるまで、ユーザ ロケールを設定しないでください。ロケール インストーラが Cisco Unified Communications Manager にロードされた後であっても、IM and Presence Service にロードされる前にユーザがユーザ ロケールを設定してしまうと、問題が発生することがあります。問題が報告された場合は、各ユーザに対し、Cisco Unified Communications Self Care Portal にサインインし、ロケールを現在の設定から [英語（English）] に変更してから適切な言語に戻すように指示することを推奨します。BAT ツールを使用してユーザ ロケールを適切な言語に同期することもできます。

手順

Step 1 cisco.com に移動し、IM and Presence Service 用のバージョンのロケール インストーラを選択します。 http://software.cisco.com/download/navigator.html?mdfid=285971059

Step 2 作業環境に適した IM and Presence ロケール インストーラのバージョンをクリックします。

Step 3 ファイルをダウンロードしたら、ハード ドライブに保存し、ファイルの保存場所をメモします。

Step 4 SFTP をサポートするサーバにこのファイルをコピーします。

Step 5 管理者のアカウントとパスワードを使用して Cisco Unified IM and Presence オペレーティング システムの管理にサインインします。

Step 6 **[ソフトウェア アップグレード（Software Upgrades）] > [インストール/アップグレード（Install/Upgrade）]**を選択します。

Step 7 ソフトウェアの入手先として [リモート ファイル システム（Remote File System）] を選択します。

Step 8 [ディレクトリ（Directory）] フィールドにファイルの保存場所（/tmp など）を入力します。

Step 9 [Server（サーバ）] フィールドに IM and Presence Service のサーバ名を入力します。

Step 10 [ユーザ名（User Name）] フィールドと [ユーザ パスワード（User Password）] フィールドに自分のユーザ名とパスワードを入力します。

Step 11 [転送プロトコル（Transfer Protocol）] で [SFTP（SFTP）] を選択します。

Step 12 [次へ（Next）] をクリックします。

Step 13 検索結果のリストから IM and Presence サービス ロケール インストーラを選択します。

Step 14 [次へ（Next）] をクリックして、インストーラ ファイルをロードし、検証します。

Step 15 ロケールのインストールが完了したら、クラスタ内の各サーバを再起動します。

Step 16 インストールされるロケールのデフォルト設定は、「英語（米国）（English United States）」です。IM and Presence Service ノードの再起動中に、必要に応じて、ダウンロードしたインストーラのロケールに合わせてブラウザの言語を変更してください。

Step 17 ユーザがサポートされている製品のロケールを選択できることを確認します。

ヒント クラスタ内のすべてのサーバに同じコンポーネントをインストールしてください。

エラー メッセージ ロケール リファレンス

ロケール インストーラをアクティブ化するときに発生する可能性のあるメッセージの説明については、次の表を参照してください。エラーが発生した場合は、インストール ログにあるメッセージを表示できます。

表 *37:* ロケール インストーラのエラー メッセージと説明

メッセージ	説明
[LOCALE] File not found: <language>_<country>_user_locale.csv, the user locale has not been added to the database.	データベースに追加するユーザ ロケール情報が格納されている CSV ファイルが見つからない場合にこのエラーが発生します。これはビルド プロセスのエラーを示しています。
[LOCALE] File not found: <country>_network_locale.csv, the network locale has not been added to the database.	データベースに追加するネットワーク ロケール情報が格納されている CSV ファイルが見つからない場合にこのエラーが発生します。これはビルド プロセスのエラーを示しています。

メッセージ	説明
[LOCALE] CSV file installer installdb is not present or not executable	installdb と呼ばれるアプリケーションが存在することを確認する必要があります。このアプリケーションはCSVファイルに含まれる情報を読み取り、それをターゲットデータベースに正しく適用します。このアプリケーションが見つからない場合、Cisco Unified Communications アプリケーションとともにインストールされなかった（ほとんどあり得ません）、削除された（可能性はあります）、またはノードにCisco Unified Communications Manager や IM and Presence Service などの Cisco Unified Communications アプリケーションがインストールされていません（最も可能性があります）。データベースに適切なレコードが格納されていないとロケールは機能しないため、ロケールのインストールは中止されます。
[LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum. [LOCALE] Could not create /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum.	これらのエラーは、システムがチェックサムファイルの作成に失敗した場合に発生します。原因としては、Java 実行ファイルの /usr/local/thirdparty/java/j2sdk/jre/bin/java が存在しない、Java アーカイブ ファイルの /usr/local/cm/jar/cmutil.jar が存在しないか損傷している、Java クラスの com.cisco.ccm.util.Zipper が存在しないか損傷していることなどが考えられます。これらのエラーが発生する場合でも、Cisco Unified Communications Manager Assistant を除いてロケールは引き続き正常に動作します。この場合、Cisco Unified Communications Manager Assistant では、ローカライズされた Cisco Unified Communications Manager Assistant ファイルの変化を検出できません。
[LOCALE] Could not find /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt in order to update Unified CM Assistant locale information.	このエラーは、適切な場所にファイルが見つからない場合に発生します。原因としては、ビルド プロセスのエラーが考えられます。
[LOCALE] Addition of <locale-installer-file-name> to the database has failed!	このエラーは、ロケールのインストール時に発生した何らかの失敗が累積されたために発生します。最終状態を示しています。

メッセージ	説明
[LOCALE] Could not locate <locale-installer-file-name>	このロケールはアップグレード中移行されません。 ダウンロードされたロケールインストーラ ファイルは、ダウンロードロケーションに置かれていません。移動または削除された可能性があります。このエラーのシビラティ（重大度）は低く、Cisco Unified Communications アプリケーションのアップグレード後にロケールインストーラを再適用するか、新しいロケールインストーラをダウンロードして適用する必要があることを示します。
[LOCALE] Could not copy <locale-installer-file-name> to migratory path. This locale will not be migrated during an upgrade!	ダウンロードされたロケールインストーラ ファイルを移行パスにコピーできません。このエラーのシビラティ（重大度）は低く、Cisco Unified Communications アプリケーションのアップグレード後にロケールインストーラを再適用するか、新しいロケールインストーラをダウンロードして適用する必要があることを示します。
[LOCALE] DRS unregistration failed	ロケール インストーラはディザスタ リカバリ システムから登録解除できませんでした。バックアップまたはリストア レコードにはロケール インストーラは含まれません。インストールのログを記録して、Cisco TAC にお問い合わせください。
[LOCALE] Backup failed!	ディザスタ リカバリ システムは、ダウンロードされたロケール インストーラ ファイルから tarball を作成できませんでした。バックアップを試みる前に、ローカルインストーラを再適用してください。 （注） システムの復元後にロケールを手動で再インストールすることもできます。
[LOCALE] No COP files found in restored tarball!	バックアップ ファイルの破損によって、ロケール インストーラ ファイルの抽出が失敗した可能性があります。 （注） ロケール インストーラを手動で再適用すると、ロケールが完全に復元されます。

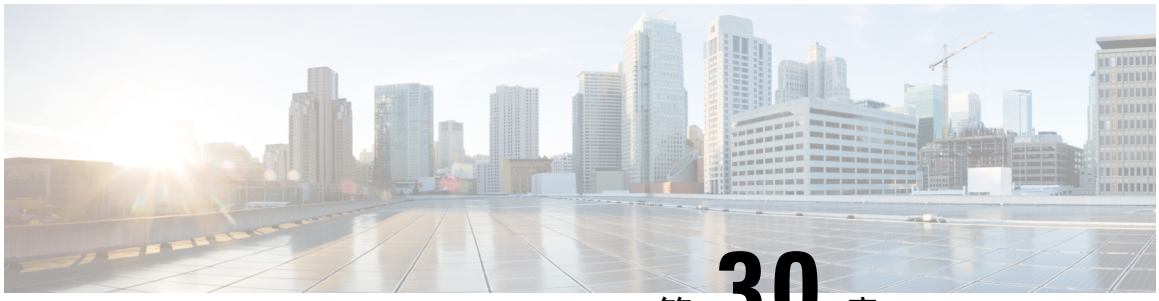
メッセージ	説明
[LOCALE] Failed to successfully reinstall COP files!	バックアップ ファイルの破損によって、ロケール インストーラ ファイルが損傷した可能性があります。 （注） ロケール インストーラを手動で再適用すると、ロケールが完全に復元されます。
[LOCALE] Failed to build script to reinstall COP files!	プラットフォームで、ロケールの再インストールに使用されるスクリプトを動的に作成できませんでした。 （注） ロケール インストーラを手動で再適用すると、ロケールが完全に復元されます。インストールのログを記録して、TAC にお問い合わせください。

ローカライズされたアプリケーション

IM and Presence Service アプリケーションはさまざまな言語をサポートします。ローカライズされたアプリケーションおよび使用可能な言語のリストについては、次の表を参照してください。

表 *38 :* ローカライズされたアプリケーションおよびサポートされる言語のリスト

インターフェイス	サポートされている言語
管理アプリケーション	
Cisco Unified CM IM and Presence の管理	中国語（中国）、英語、日本語（日本）、韓国語（韓国）
Cisco Unified IM and Presence オペレーティング システム	中国語（中国）、英語、日本語（日本）、韓国語（韓国）



第 30 章

サーバの管理

サーバの管理の概要

この章では、導入されたシステムのサーバの詳細を編集する方法について説明します。これには、新しいノードのクラスタへの割り当て、クラスタからのノードの削除、プレゼンス ステータスの表示、およびサーバ アドレスの詳細情報の変更が含まれます。

サーバの IP アドレスの変更

稼働中のシステムがあり、サーバのアドレス指定に以下の変更を加える必要がある場合は、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlの *Cisco Unified Communications Manager* および *IM and Presence Service* アドレスとホスト名の変更の手順を参照してください。

これは、以下のタイプのアドレス変更に適用されます。

- サーバの IP アドレスの変更
- サーバのホスト名の変更
- ノード名の変更（たとえば、IP アドレスを使用してノード名を定義しており、そのホスト名を使用する場合）。
- IM and Presence Service のデフォルト ドメインの変更

クラスタからの IM and Presence ノードの削除

プレゼンス冗長グループおよびクラスタから IM and Presence Service ノードを安全に削除する必要がある場合は、この手順に従います。

⚠

注意　ノードを削除すると、そのプレゼンス冗長グループの残りのノードで、ユーザに対するサービスが中断されます。この手順は必ず、メンテナンス期間中に実行してください。

手順

Step 1　**[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [システム（System）] > [プレゼンス冗長グループ（Presence Redundancy Groups）]**ページで、高可用性が有効な場合は無効にします。

Step 2　**[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [ユーザ管理（User Management）] > [プレゼンスユーザの割り当て（Assign Presence Users）]**ページで、削除するノードからすべてのユーザの割り当てを解除するか、移動します。

Step 3　プレゼンス冗長グループからノードを削除するには、プレゼンス冗長グループの [プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ページの [プレゼンスサーバ（Presence Server）] ドロップダウン リストから、[未選択（Not-Selected）] を選択します。ノードの割り当て解除の結果としてプレゼンス冗長グループ内のサービスが再起動されることを示す警告ダイアログ ボックスが表示されたら、[OK] を選択します。

（注）　プレゼンス冗長グループから直接パブリッシャノードを削除することはできません。パブリッシャノードを削除するには、まずパブリッシャノードからユーザの割り当てを解除し、プレゼンス冗長グループを完全に削除します。

ただし、削除された IM and Presence ノードをクラスタに再び追加することができます。削除されたノードを追加する方法の詳細に削除したサーバをクラスタに戻す（391 ページ）ついては、を参照してください。このシナリオでは、Cisco DefaultCUPSubcluster CM Administration コンソールの [**System > server**] 画面で、削除されたパブリッシャノードがサーバに再び追加されると、 が自動的に作成されます。

Step 4　Cisco Unified CM Administration で、**[システム（System）] > [サーバ（Server）]** から未割り当てのノードを削除します。この操作は取り消せないことを示す警告ダイアログ ボックスが表示されたら、[OK] をクリックします。

Step 5　割り当てを解除したノードのホスト VM またはサーバをシャットダウンします。

Step 6　すべてのノードの **Cisco XCP Router** を再起動します。

削除したサーバをクラスタに戻す

Unified Communications Manager Administration から後続のノード（サブスクライバ）を削除してそれをクラスタに戻す場合に、次の手順を実行します。

手順

Step 1 Cisco Unified Communications Manager Administration で、**[システム（System）]** > **[サーバ（Server）]** を選択してサーバを追加します。

Step 2 後続のノードを Cisco Unified Communications Manager Administration に追加したら、シスコが提供しているソフトウェア キットに付属しているご使用のバージョン用のディスクを使用して、サーバ上でインストールを実行します。

ヒント インストールするバージョンが、パブリッシャ ノード上で動作しているバージョンと一致することを確認します。パブリッシャ上で実行されているバージョンがインストール ファイルと一致しない場合は、インストール プロセス中に [インストール中にアップグレード（Upgrade During Install）] オプションを選択します。インストールの詳細については、『*Installation Guide for Cisco Unified Communications Manager and the IM and Presence Servic*』を参照してください。

Step 3 Cisco UnifiedCM をインストールしたら、その Cisco UnifiedCM のバージョンをサポートしているインストール マニュアルの説明に従って、後続のノードを設定します。

Step 4 Cisco Unified Reporting、RTMT、または CLI にアクセスして、データベース レプリケーションが既存のノード間で発生していることを確認します。必要に応じて、ノード間のデータベース レプリケーションを修復します。

インストール前のクラスタへのノードの追加

ノードをインストールする前に、Cisco Unified Communications Manager Administration を使用して、新しいノードをクラスタに追加します。ノードの追加時に選択するサーバ タイプは、インストールしたサーバ タイプと一致する必要があります。

新しいノードをインストールする前に、Cisco Unified Communications Manager Administration を使用して、最初のノードで新しいノードを設定する必要があります。クラスタにノードをインストールするには、『*Cisco Unified Communications ManagerInstallation Guide*』を参照してください。

Cisco Unified Communications Manager のビデオ/音声サーバでは、Cisco Unified Communications Manager ソフトウェアの初期インストール中に追加した最初のサーバーがパブリッシャ ノードに指定されます。後続のすべてのサーバインストールまたは追加は、サブスクライバ ノードに指定されます。クラスタに追加した最初の Cisco Unified Communications Manager IM and Presence ノードが、IM and Presence Service データベース パブリッシャノードに指定されます。

（注） サーバの追加後は、Cisco Unified Communications Manager Administration を使用して、サーバ タイプを変更できなくなります。既存のサーバ インスタンスを削除してから、再度、新しいサーバを追加して、正しいサーバ タイプ設定を選択する必要があります。

手順

Step 1 **[システム（System）]** > **[サーバ（Server）]** を選択します。

[サーバの検索/一覧表示（Find and List Servers）] ウィンドウが表示されます。

Step 2 [新規追加（Add New）] をクリックします。

[サーバの設定 - サーバを追加（Server Configuration - Add a Server）] ウィンドウが表示されます。

Step 3 [サーバ タイプ（Server Type）] ドロップダウン リスト ボックスで、追加するサーバ タイプを選択してから、[次へ（Next）] をクリックします。

- CUCM ビデオ/音声
- CUCM IM and Presence

Step 4 [サーバの設定（Server Configuration）] ウィンドウで、適切なサーバ設定を入力します。

サーバ設定フィールドの説明については、「Server Settings」を参照してください。

Step 5 [保存（Save）] をクリックします。

プレゼンス サーバのステータスの表示

IM and Presence Service ノードの重要なサービスのステータスと自己診断テスト結果を確認するには、Cisco Unified Communications Manager Administration を使用します。

手順

Step 1 **[システム（System）]** > **[サーバ（Server）]** を選択します。

[サーバの検索/一覧表示（Find and List Servers）] ウィンドウが表示されます。

Step 2 サーバの検索パラメータを選択し、**[検索（Find）]** をクリックします。

一致するレコードが表示されます。

Step 3 **[サーバーの検索/一覧表示（Find and List Servers）]** ウィンドウに表示される IM and Presence サーバを選択します。

[サーバーの設定（Server Configuration）] ウィンドウが表示されます。

Step 4 **[サーバーの設定（Server Configuration）]** ウィンドウの IM and Presence サーバ情報のセクションで、プレゼンス サーバ ステータスのリンクをクリックします。

サーバーの [ノードの詳細（Node Details）] ウィンドウが表示されます。

ハイ アベイラビリティでのサービスの再起動

ハイアベイラビリティを無効にしてから Cisco XCP ルータ、Cisco Presence エンジン、またはサーバ自体を再起動する必要があるシステム設定変更またはシステムアップグレードを行う場合は、Cisco Jabber セッションのために十分な時間を確保する必要があります。ハイアベイラビリティを有効にする前に再作成されます。十分な時間を確保しない場合、セッションが作成されていない Jabber クライアントでプレゼンスは機能しません。

次のプロセスに従ってください。

手順

Step 1 変更を加える前に、Cisco Unified CM IM and Presence 管理ウィンドウ (**システム** > **プレゼンストポロジ**) の [**プレゼンストポロジ (プレゼンストポロジ)**] ウィンドウを確認します。各プレゼンス冗長グループの各ノードに割り当てられたユーザ数を記録します。

Step 2 各プレゼンス冗長グループのハイアベイラビリティを無効にし、新しい HA 設定が同期されるまで少なくとも2分間待機します。

Step 3 更新には、次のいずれかを実行する必要があります。

- Cisco XCP ルータの再起動
- Cisco Presence Engine の再起動
- サーバを再起動します。

Step 4 再起動後、すべてのノードでアクティブなセッションの数をモニタします。

Step 5 各ノードで、各ノードで`show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI コマンドを実行し、各ノードでアクティブなセッションの数を確認します。アクティブセッションの数は、割り当てられたユーザのステップ1で記録した番号と一致している必要があります。すべてのセッションが再開されるまで15分以上かかりません。

Step 6 すべてのセッションが作成されたら、プレゼンス冗長グループ内でハイアベイラビリティを有効にすることができます。

（注） 30分が経過し、アクティブセッションがまだ作成されていない場合は、Cisco Presence エンジンを再起動します。それでも問題が解決しない場合は、システムの問題が大きくなります。

（注） Cisco XCP ルータや Cisco Presence Engine、あるいはその両方を連続して再起動することは推奨しません。ただし、以下のように再起動する必要がある場合は、最初のサービスを再起動し、JSMのすべてのセッションが再作成されるまで待機します。JSMセッションがすべて作成されたら、2 つ目の再起動を実行します。

ホスト名の設定

次の表に、Unified Communications Manager サーバのホスト名を設定できる場所、ホスト名として指定できる文字数、および推奨されるホスト名の先頭文字と最終文字を示します。ホスト名を正しく設定しないと、Unified Communications Manager の一部のコンポーネント（オペレーティングシステム、データベース、インストールなど）が期待通りに機能しない可能性があります。

表 *39 : Cisco Unified Communications Manager* におけるホスト名の設定

ホスト名の場所	許可された設定	許容文字数	推奨されるホスト名の最初の文字	推奨されるホスト名の最後の文字
[ホスト名/IP アドレス（Host Name/ IP Address）] フィールド Cisco Unified Communications Manager Administration の **[システム（System）] > [サーバ（Server）]**	クラスタ内のサーバのホスト名を追加または変更できます。	2 ～ 63	アルファベット	英数字
[ホスト名（Hostname）] フィールド Cisco Unified Communications Manager インストール ウィザード	クラスタ内のサーバのホスト名を追加できます。	1 ～ 63	アルファベット	英数字
[ホスト名（Hostname）] フィールド Cisco Unified Communications オペレーティング システムの **[設定（Settings）] > [IP] > [イーサネット（Ethernet）]**	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1 ～ 63	アルファベット	英数字
set network hostname hostname コマンドラインインターフェイス	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1 ～ 63	アルファベット	英数字

ヒント　このホスト名は、ARPANET ホスト名の規則に従う必要があります。ホスト名の先頭文字と最終文字の間には、英数文字とハイフンを入力できます。

いずれかの場所でホスト名を設定する前に、次の情報を確認してください。

- [サーバの設定（Server Configuration）] ウィンドウの [ホスト名/IP アドレス（Host Name/IP Address）] フィールドは、デバイスとサーバ間、アプリケーションとサーバ間、および異なるサーバ間の通信をサポートします。このフィールドには、ドット区切り形式の IPv4 アドレスまたはホスト名を入力できます。

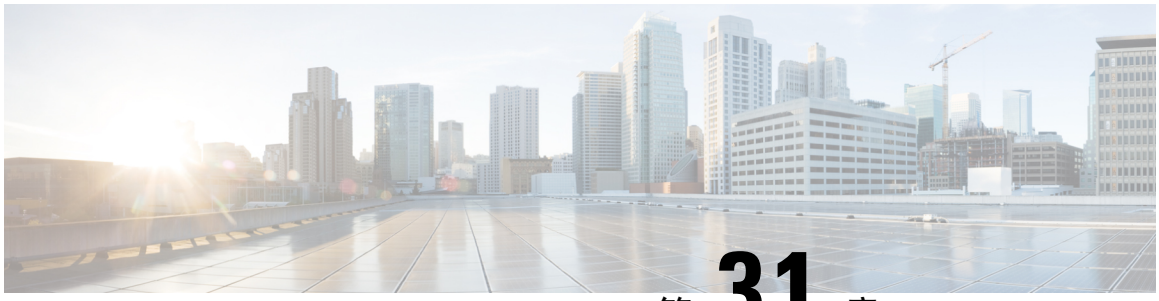
  Unified Communications Manager パブリッシャ ノードをインストールした後は、パブリッシャのホスト名がこのフィールドに自動的に表示されます。Unified Communications Managerサブスクライバ ノードをインストールする前に、Unified Communications Manager パブリッシャ ノードでこのフィールドにサブスクライバ ノードの IP アドレスまたはホスト名を入力してください。

  このフィールドにホスト名を設定できるのは、Unified Communications Manager が DNS サーバにアクセスしてホスト名を IP アドレスに解決できる場合のみです。DNS サーバに Cisco Unified Communications Manager の名前とアドレスの情報が設定されていることを確認してください。

ヒント　DNS サーバに Unified Communications Manager の情報を設定するのに加えて、Cisco Unified Communications Manager のインストール時に DNS 情報を入力します。

- Unified Communications Manager パブリッシャ ノードのインストール時に、ネットワーク情報を設定するために（つまり、スタティック ネットワークを使用する場合に）パブリッシャ サーバのホスト名（必須）と IP アドレスを入力します。

  Unified Communications Manager サブスクライバ ノードのインストール時には、Unified Communications Manager パブリッシャ ノードのホスト名と IP アドレスを入力して、Unified Communications Manager がネットワークの接続性およびパブリッシャとサブスクライバ間の検証を確認できるようにしてください。さらに、サブスクライバ ノードのホスト名と IP アドレスも入力する必要があります。Unified Communications Manager のインストール時にサブスクライバ サーバのホスト名の入力を求められた場合は、Cisco Unified Communications Manager Administration の（[ホスト名/IP アドレス（Host Name/IP Address）] フィールドでサブスクライバ サーバのホスト名を設定した場合に）[サーバの設定（Server Configuration）] ウィンドウに表示される値を入力します。



第 31 章

システムのバックアップ

バックアップの概要

定期的にバックアップを行うことを推奨します。ディザスタ リカバリ システム（DRS）を使用して、クラスタ内のすべてのサーバのデータを完全にバックアップできます。自動バックアップをセットアップすることも、任意の時点でバックアップを起動することもできます。

ディザスタ リカバリ システムで実行するバックアップは、クラスタ レベルであり、Cisco Unified Communications Manager クラスタ内のすべてのサーバのバックアップを 1 箇所に集め、バックアップ データを物理的なストレージ デバイスにアーカイブします。バックアップ ファイルは暗号化され、システム ソフトウェアによってだけ開くことができます。

DRS は、プラットフォームのバックアップ/復元の一環として、独自の設定（バックアップ デバイス設定およびスケジュール設定）を復元します。DRS は drfDevice.xml ファイルと drfSchedule.xml ファイルをバックアップおよび復元します。これらのファイルとともにサーバを復元するときは、DRS バックアップ デバイスおよびスケジュールを再設定する必要がありません。

システム データを復元するときには、クラスタ内のどのノードを復元するかを選択できます。

ディザスタ リカバリ システムには、次の機能があります。

- バックアップおよび復元タスクを実行するためのユーザ インターフェイス。
- バックアップ機能を実行するための分散システム アーキテクチャ。
- スケジュール バックアップまたは手動（ユーザが起動する）バックアップ。
- リモート SFTP サーバへのバックアップのアーカイブ。

表に、ディザスタ リカバリ システム（DRS）によるバックアップ/復元が可能な機能とコンポーネントを示します。各機能を選択すると、各機能のすべてのコンポーネントが自動的にバックアップされます。

表 *40 : Cisco Unified CM* の機能とコンポーネント

機能	コンポーネント
CCM：Unified Communications Manager	Unified Communications Manager データベース
	プラットフォーム
	サービサビリティ
	保留音（MOH）
	Cisco Emergency Responder
	Bulk Tool（BAT）
	設定
	電話デバイス ファイル（TFTP）
	syslogagt（SNMP syslog エージェント）
	cdpagent（SNMP cdp エージェント）
	tct（トレース収集ツール）
	コール詳細レコード（CDR）
	CDR Reporting and Analysis（CAR）

表 *41 : IM and Presence* の機能とコンポーネント

機能	コンポーネント
IM and Presence Service	IM and Presence データベース
	syslogagt（SNMP syslog エージェント）
	cdpagent（SNMP cdp エージェント）
	Platform
	レポーター（有用性レポーター）
	CUP SIP プロキシ
	XCP
	CLM
	Bulk Tool（BAT）
	設定
	tct（トレース収集ツール）

バックアップの前提条件

- バージョンの要件を満たしていることを確認してください。
  - すべての Cisco Unified Communications Manager クラスタ ノードは、同じバージョンの Cisco Unified Communications Manager アプリケーションを実行している必要があります。
  - すべての IM and Presence Service クラスタ ノードは、同じバージョンの IM and Presence Service アプリケーションを実行している必要があります。
  - バックアップ ファイルに保存されているソフトウェア バージョンが、クラスタ ノードで実行されるバージョンと同じでなければなりません。

バージョンの文字列全体が一致している必要があります。たとえば、IM and Presence データベース パブリッシャ ノードがバージョン 11.5.1.10000-1 の場合、すべての IM and Presence サブスクライバ ノードは 11.5.1.10000-1 であり、バックアップ ファイルに保存されているバージョンも 11.5.1.10000-1 でなければなりません。現在のバージョンと一致しないバックアップ ファイルからシステムを復元しようすると、復元は失敗します。バックアップ ファイルに保存されているバージョンが、クラスタ ノードで実行されているバージョンと一致するよう、ソフトウェア バージョンをアップグレードしたら常にシステムをバックアップするようにしてください。

- DRS暗号化は、クラスタセキュリティパスワードに依存することに留意してください。バックアップの実行中に、DRSは暗号化のためにランダムパスワードを生成し、そのランダムパスワードをクラスタセキュリティパスワードを使用して暗号化します。バックアップを実行した後、復元を行うまでの間にクラスタ セキュリティ パスワードが変更された場合、そのバックアップ ファイルを使用してシステムを復元するには、バックアップを実行した時点でのパスワードを把握していなければなりません。あるいは、セキュリティパスワードを変更/リセットした直後にバックアップを作成するようにしてください。
- リモート デバイスをバックアップする必要がある場合は、必ず SFTP サーバを設定する必要があります。利用可能なSFTPサーバの詳細については、次の項を参照してください。リモート バックアップ用 SFTP サーバ （407 ページ）

バックアップ タスク フロー

次のタスクを実行して、バックアップを設定して実行します。バックアップの実行中は OS 管理タスクを実行しないでください。これは、ディザスタ リカバリ システムがプラットフォーム API をロックすることにより、すべてのOS管理要求をブロックするためです。ただし、CLIベースのアップグレード コマンドしかプラットフォーム API ロッキング パッケージを使用しないため、ディザスタ リカバリ システムはほとんどの CLI コマンドを妨害しません。

手順

	コマンドまたはアクション	目的
Step 1	バックアップ デバイスの設定 （401 ページ）	データをバックアップするデバイスを指定します。
Step 2	バックアップ ファイルのサイズの予測 （402 ページ）	SFTP デバイス上で作成されるバックアップ ファイルのサイズを見積もります。
Step 3	次のいずれかのオプションを選択します。 • スケジュール バックアップの設定 （403 ページ） • 手動バックアップの開始 （404 ページ）	スケジュールに従ってデータをバックアップするためのバックアップ スケジュールを作成します。 または、手動バックアップを実行します。
Step 4	現在のバックアップ ステータスの表示 （405 ページ）	これはオプションです。バックアップのステータスをチェックします。バックアップの実行中、現在のバックアップ ジョブのステータスを確認できます。
Step 5	バックアップ履歴の表示 （406 ページ）	これはオプションです。バックアップ履歴の表示

バックアップ デバイスの設定

最大 10 個のバックアップ デバイスを設定できます。バックアップ ファイルを保存する場所を設定するには、次の手順を実行します。

始める前に

- バックアップ ファイルを保存するために SFTP サーバにディレクトリ パスへの書き込みアクセス権があることを確認します。
- DRS マスター エージェントがバックアップ デバイスの設定を検証するときに、ユーザ名、パスワード、サーバ名とディレクトリ パスが有効であることを確認します。

（注） バックアップはネットワーク トラフィックが少なくなる時間帯にスケジューリングしてください。

手順

Step 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）]>[バックアップ デバイス（Backup Device）]** の順に選択します。

Step 2 [バックアップ デバイス リスト（Backup Device List）] ウィンドウで、次のいずれかを実行します。

- 新しいデバイスを設定するには、[新規追加（Add New）] をクリックします。
- 既存のバックアップ デバイスを編集するには、検索条件を入力し、[検索（Find）]、次に [選択項目の編集（Edit Selected）] をクリックします。
- バックアップ デバイスを削除するには、[バックアップ デバイス（Backup Device）] リストでバックアップ デバイスを選択してから [選択項目の削除（Delete Selected）] をクリックします。

バックアップ スケジュールにバックアップ デバイスとして設定されているバックアップ デバイスは削除できません。

Step 3 [バックアップ デバイス名（Backup device name）] フィールドにバックアップ名を入力します。

バックアップ デバイス名には、英数字、スペース（）、ダッシュ（-）、およびアンダースコア（_）だけを使用します。それ以外の文字は使用しないでください。

Step 4 [接続先の選択（Select Destination）] 領域の [ネットワーク ディレクトリ（Network Directory）] で、次を実行します。

- [ホスト名/IP アドレス（Host name/IP Address）] フィールドに、ネットワーク サーバのホスト名または IP アドレスを入力します。
- [パス名（Path name）] フィールドに、バックアップ ファイルを格納するディレクトリ パスを入力します。

- [ユーザ名（User name）] フィールドに、有効なユーザ名を入力します。
- [パスワード（Password）] フィールドに、有効なパスワードを入力します。
- [ネットワーク ディレクトリに保存するバックアップ数（Number of backups to store on Network Directory）] ドロップダウン リストから、バックアップの必要数を選択します。

Step 5 [保存（Save）] をクリックします。

次のタスク

バックアップ ファイルのサイズの予測 （402 ページ）

バックアップ ファイルのサイズの予測

1 つまたは複数の選択した機能のバックアップ履歴が存在する場合に限り、Cisco Unified Communications Manager は、バックアップ tar のサイズを予測します。

計算されたサイズは正確な値ではなく、バックアップ tar の予測サイズです。サイズは前のバックアップの実際のバックアップ サイズに基づいて計算され、設定が前回のバックアップ以降変更された場合は異なることがあります。

この手順は、前回のバックアップが存在する場合にのみ使用でき、初めてシステムをバックアップする場合は使用できません。

SFTP デバイスに保存されているバックアップ tar のサイズを予測するには、次の手順に従ってください。

手順

Step 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）] > [手動バックアップ（Manual Backup）]** の順に選択します。

Step 2 [機能の選択（Select Features）] 領域でバックアップする機能を選択します。

Step 3 選択した機能のバックアップの予測サイズを表示するには、[サイズの予測（Estimate Size）] を選択します。

次のタスク

システムをバックアップするには、次のいずれかの手順を実行します。

- スケジュール バックアップの設定 （403 ページ）
- 手動バックアップの開始 （404 ページ）

スケジュール バックアップの設定

最大 10 個のバックアップ スケジュールを作成できます。各バックアップ スケジュールには、自動バックアップのスケジュール、バックアップする機能セット、保存場所など、独自のプロパティがあります。

バックアップ .tar ファイルはランダムに生成されるパスワードで暗号化されるということに注意してください。このパスワードは、クラスタセキュリティパスワードで暗号化され、バックアップ .tar ファイルとともに保存されます。このセキュリティ パスワードは忘れないように記憶しておくか、またはセキュリティ パスワードを変更またはリセットしたらすぐにバックアップを作成する必要があります。

注意　コール処理が中断してサービスに影響が及ばないように、バックアップはオフピーク時間中にスケジュールしてください。

始める前に

バックアップ デバイスの設定 （401 ページ）

手順

Step 1　ディザスタ リカバリ システムで、[バックアップ スケジューラ（Backup Scheduler）] を選択します。

Step 2　[スケジュール リスト（Schedule List）] ウィンドウで、新規スケジュールを追加するか、または既存のスケジュールを編集します。

- 新規スケジュールを作成するには、[新規追加（Add New）] をクリックします。
- 既存のスケジュールを設定するには、[スケジュール リスト（Schedule List）]列でその名前をクリックします。

Step 3　[スケジューラ（scheduler）] ウィンドウで、[スケジュール名（Schedule Name）] フィールドにスケジュール名を入力します。

（注）　デフォルトのスケジュールの名前は変更できません。

Step 4　[バックアップ デバイスの選択（Select Backup Device）] 領域でバックアップ デバイスを選択します。

Step 5　[機能の選択（Select Features）] 領域でバックアップする機能を選択します。少なくとも 1 つの機能を選択する必要があります。

Step 6　[バックアップの開始時刻（Start Backup at）] 領域でバックアップを開始する日付と時刻を選択します。

Step 7　[頻度（Frequency）] 領域でバックアップを行う頻度を選択します。頻度は、[一度（Once）]、[日次（Daily）]、[週次（Weekly）]、[月次（Monthly）] に設定できます。[週次（Weekly）] を選択した場合は、バックアップを行う週の曜日も選択できます。

ヒント　バックアップ頻度を火曜日から土曜日までの [週次（Weekly）] に設定するには、[デフォルトの設定（Set Default）] をクリックします。

Step 8　これらの設定を更新するには、[保存（Save）] をクリックします。

Step 9　次のいずれかのオプションを選択します。

- 選択したスケジュールをイネーブルにするには、[選択されたスケジュールの有効化（Enable Selected Schedules）] をクリックします。
- 選択したスケジュールをディセーブルにするには、[選択されたスケジュールの無効化（Disable Selected Schedules）] をクリックします。
- 選択したスケジュールを削除するには、[選択項目の削除（Delete Selected）] をクリックします。

Step 10　スケジュールを有効にするには、[スケジュールの有効化（Enable Schedule）] をクリックします。

設定した時刻になると自動的に次のバックアップが実行されます。

（注）　クラスタ内のすべてのサーバーが、同じバージョンの Cisco Unified Communications Manager または Cisco IM and Presence サービスを実行し、ネットワークから到達可能であることを確認します。スケジュールされたバックアップの時刻にサーバに到達できないと、そのサーバーはバックアップされません。

次のタスク

次の手順を実行します。

- バックアップ ファイルのサイズの予測（402 ページ）
- （省略可）現在のバックアップ ステータスの表示（405 ページ）

手動バックアップの開始

始める前に

- バックアップ ファイルの格納場所としてネットワーク デバイスを使用していることを確認します。Unified Communications Manager の仮想化展開では、テープ ドライブによるバックアップ ファイルの保存はサポートされません。
- Cisco Unified Communications Manager または IM and Presence Service のインストールされているバージョンが、すべてのクラスタ ノードで同じであることを確認します。
- バックアップ プロセスは、リモート サーバに利用可能な容量がないためや、ネットワーク接続が中断されたために失敗することがあります。バックアップが失敗する原因となった問題に対処した後、新規のバックアップを開始する必要があります。
- ネットワークの中断がないことを確認してください。

- バックアップ デバイスの設定（401 ページ）
- バックアップ ファイルのサイズの予測（402 ページ）
- クラスタセキュリティパスワードのレコードがあることを確認します。このバックアップの完了後に、クラスタセキュリティパスワードを変更した場合は、パスワードを認識している必要があります。パスワードを認識していないと、バックアップ ファイルを使用してシステムを復元できなくなります。

（注） バックアップが実行されている間は、Disaster Recovery System がプラットフォーム API をロックしてすべての要求をブロックするため、Cisco Unified OS の管理または Cisco Unified IM and Presence OS の管理でタスクを実行することはできません。ただし、ディザスタ リカバリ システムは、CLI ベースのアップグレード コマンドだけがプラットフォーム API ロッキング パッケージを使用するため、ほとんどの CLI コマンドをブロックしません。

手順

Step 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）] > [手動バックアップ（Manual Backup）]** の順に選択します。

Step 2 [手動バックアップ（Manual Backup）] ウィンドウで、[バックアップ デバイス名（Backup Device Name）] 領域を選択します。

Step 3 [機能の選択（Select Features）] 領域から機能を選択します。

Step 4 [バックアップの開始（Start Backup）] をクリックします。

次のタスク

（省略可） 現在のバックアップ ステータスの表示（405 ページ）

現在のバックアップ ステータスの表示

現在のバックアップ ジョブのステータスを確認するには、次の手順を実行します。

注意 リモート サーバへのバックアップが 20 時間以内に完了しないとバックアップ セッションがタイムアウトするため、新規バックアップを開始する必要があります。

手順

Step 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）] > [現在のステータス（Current Status）]** の順に選択します。

Step 2 バックアップ ログ ファイルを表示するには、ログファイル名リンクをクリックします。

Step 3 現在のバックアップをキャンセルするには、[バックアップのキャンセル（Cancel Backup）] をクリックします。

（注） 現在のコンポーネントがバックアップ操作を完了した後、バックアップがキャンセルされます。

次のタスク

バックアップ履歴の表示 （406 ページ）

バックアップ履歴の表示

バックアップ履歴を参照するには、次の手順を実行します。

手順

Step 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）] > [履歴（History）]** の順に選択します。

Step 2 [バックアップ履歴（Backup History）] ウィンドウで、ファイル名、バックアップ デバイス、完了日、結果、バージョン、バックアップされている機能、失敗した機能など、実行したバックアップを表示できます。

（注） [バックアップ履歴（Backup History）] ウィンドウには、最新の 20 個のバックアップ ジョブだけが表示されます。

バックアップの連携動作と制約事項

• バックアップの制約事項 （407 ページ）

バックアップの制約事項

バックアップには、次の制約事項が適用されます。

表 *42 :* バックアップの制約事項

制限事項	説明
クラスタ セキュリティ パスワード	クラスタ セキュリティ パスワードを変更したら、必ずバックアップを実行することを推奨します。 バックアップ暗号化では、バックアップ ファイルのデータを暗号化する際にクラスタセキュリティパスワードを使用します。バックアップ ファイルの作成後にクラスタ セキュリティ パスワードを編集すると、古いパスワードを忘れてしまった場合に、そのバックアップ ファイルを使用してデータを復元できなくなります。
証明書の管理	ディザスタ リカバリ システム（DRS）は、マスター エージェントとローカル エージェントとの間で SSL ベースの通信を使用して、Cisco Unified Communications Manager クラスタ ノード間のデータの認証および暗号化を行います。DRS は、IPSec 証明書を使用して、公開キー/秘密キーの暗号化を行います。証明書管理ページから IPSEC 信頼ストア（hostname.pem）ファイルを削除すると、DRS が想定どおりに機能しなくなることに注意してください。IPSEC 信頼ファイルを手動で削除するときは、IPSEC 証明書を IPSEC 信頼に必ずアップロードしてください。詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*Security Guide for Cisco Unified Communications Manager*』の「証明書管理」の項を参照してください。

リモート バックアップ用 SFTP サーバ

データをネットワーク上のリモート デバイスにバックアップするには、SFTP サーバを用意して必要な設定を行う必要があります。シスコは内部テストでは、Cisco TAC にサポートされている、シスコ提供の Cisco Prime Collaboration Deployment（PCD）上で SFTP サーバを使用します。SFTP サーバ オプションの概要については、次の表を参照してください。

以下の表示に記載されている情報を参考に、システムで使用する SFTP サーバ ソリューションを決定してください。

表 *43 : SFTP* サーバ情報

SFTP サーバ	情報
Cisco Prime Collaboration Deployment の SFTP サーバ	このサーバーはシスコが提供およびテストしたSFTPサーバのみであり、Cisco TAC がサポートします。 バージョンの互換性は、使用している Unified Communications Manager および Cisco Prime Collaboration Deployment のバージョンに依存します。バージョン（SFTP）または Unified Communications Manager をアップグレードする前に、『Cisco Prime Collaboration Deployment Administration Guide』を参照して、互換性のあるバージョンであることを確認してください。
テクノロジー パートナーの SFTP サーバ	これらのサーバーはサードパーティが提供およびテストしたものです。バージョンの互換性は、サードパーティによるテストに依存します。テクノロジー パートナーの SFTP サーバまたは Unified Communications Manager をアップグレードする場合、テクノロジー パートナーのページで、互換性のあるバージョンを確認してください。 https://marketplace.cisco.com
他のサードパーティの SFTP サーバ	これらのサーバーはサード パーティが提供するものであり、Cisco TAC はこれらのサーバを正式にサポートしていません。 バージョンの互換性は、SFTP バージョンと Unified Communications Manager バージョンの互換性を確立するためのベストエフォートに基づきます。 （注） これらの製品がシスコでテストされていない場合、シスコはその機能を保証することができません。Cisco TAC は、これらの製品をサポートしていません。完全にテストされてサポートされる SFTP ソリューションとしては、Cisco Prime Collaboration Deployment またはテクノロジー パートナーの SFTP サーバを利用してください。

暗号サポート

Unified Communications Manager 11.5 では、Unified Communications Manager は SFTP 接続用に次の CBC および CRT 暗号をアドバタイズします。

- aes128-cbc
- 3des-cbc
- aes128-ctr
- aes192-ctr

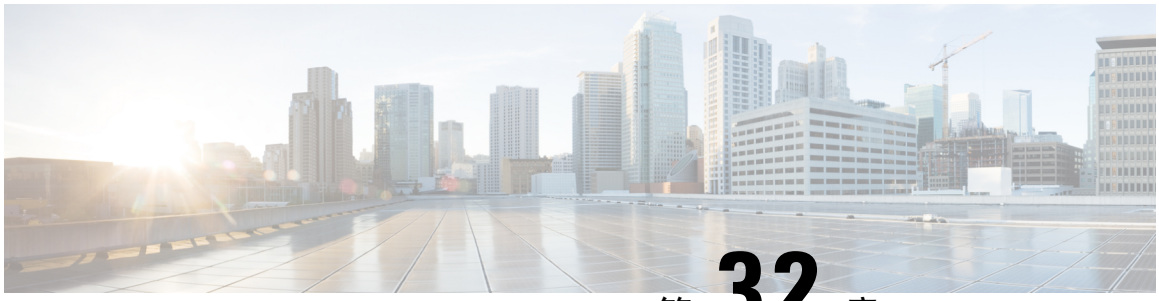
- aes256-ctr

（注） Unified Communications Manager との通信のために、バックアップ SFTP サーバーがこれらの暗号のいずれかをサポートしていることを確認してください。

Unified Communications Manager 12.0 リリース以降では、CBC 暗号はサポートされていません。Unified Communications Manager は、次の CTR 暗号のみをサポートおよびアドバタイズします。

- aes256-ctr
- aes128-ctr
- aes192-ctr

（注） バックアップ SFTP サーバーが Unified Communications Manager との通信のためにこれらの CTR 暗号のいずれかをサポートしていることを確認します。



第 32 章

システムの復元

復元の概要

ディザスタ リカバリ システム（DRS）には、システムを復元するプロセスを実行するためのガイドとなるウィザードが用意されています。

バックアップ ファイルは暗号化されており、それらを開いてデータを復元できるのはDRS システムのみです。ディザスタ リカバリ システムには、次の機能があります。

- 復元タスクを実行するためのユーザ インターフェイス。
- 復元機能を実行するための分散システム アーキテクチャ。

マスター エージェント

クラスタの各ノードで自動的にマスターエージェント サービスが起動されますが、マスターエージェントはパブリッシャ ノード上でのみ機能します。サブスクライバ ノード上のマスター エージェントは、何の機能も実行しません。

ローカル エージェント

サーバには、バックアップおよび復元機能を実行するローカル エージェントが搭載されています。

マスター エージェントを含むノードをはじめ、Cisco Unified Communications Manager クラスタ内の各ノードには、バックアップおよび復元機能を実行するために独自のローカル エージェントが必要です。

（注） デフォルトでは、ローカル エージェントは IM and Presence ノードをはじめ、クラスタ内の各ノードで自動的に起動されます。

復元の前提条件

- バージョンの要件を満たしていることを確認してください。
  - すべての Cisco Unified Communications Manager クラスタ ノードは、同じバージョンの Cisco Unified Communications Manager アプリケーションを実行している必要があります。
  - すべての IM and Presence Service クラスタ ノードは、同じバージョンの IM and Presence Service アプリケーションを実行している必要があります。
  - バックアップ ファイルに保存されているバージョンが、クラスタ ノードで実行されるバージョンと同じでなければなりません。

  バージョンの文字列全体が一致している必要があります。たとえば、IM and Presence データベース パブリッシャ ノードがバージョン 11.5.1.10000-1 の場合、すべての IM and Presence サブスクライバ ノードは 11.5.1.10000-1 であり、バックアップ ファイルに保存されているバージョンも 11.5.1.10000-1 でなければなりません。現在のバージョンと一致しないバックアップ ファイルからシステムを復元しようすると、復元は失敗します。
- サーバの IP アドレス、ホスト名、DNS 設定および導入タイプが、バックアップ ファイルに保存されている IP アドレス、ホスト名、DNS 設定および導入タイプと一致していることを確認します。
- バックアップを実行した後にクラスタ セキュリティ パスワードを変更した場合、元のパスワードのレコードを記録しておきます。元のパスワードが分からなければ、復元は失敗します。
- クラスターで IPsec ポリシーが有効になっている場合は、復元操作を開始する前に無効にしてください。

復元後に SAML SSO を再度有効にする

重要 このセクションは、リリース 12.5(1)SU7 にのみ適用されます。

DRS を使用してシステムを復元した後、クラスタ内のいずれかのノードで SAML SSO が断続的に無効化されることがあります。影響を受けるノードで SAML SSO を再度有効にするには、以下を実行する必要があります：

1. Cisco Unified CM の管理で、**[システム（System）]** > **[SAML シングルサインオン（SAML Single Sign-On）]** を選択します。
2. **[すべての無効なサーバーの修正（Fix All Disabled Servers）]** をクリックします。

   [SAML シングルサインオンの設定（SAML Single Sign-On Configuration）] ウィンドウが表示されるので、**[次へ（Next）]** をクリックします。
3. [SSO テストを実行（Run SSO Test）] をクリックします。
4. **[SSO のテストに成功しました!（SSO Test Succeeded!）]** というメッセージが表示されたら、ブラウザウィンドウを閉じ、**[終了（Finish）]** をクリックします。

（注） SAML SSO を再度有効にするプロセス中に Cisco Tomcat が再起動します。SAML SSO がすでに有効になっているノードには影響しません。

復元タスク フロー

復元プロセス中、[Cisco Unified CM の管理（Cisco Unified Communications Manager OS Administration）] または [Cisco Unified CM IM and Presence OS の管理（Cisco Unified IM and Presence OS Administration）] に関するタスクを実行しないでください。

手順

	コマンドまたはアクション	目的
Step 1	最初のノードのみの復元 （414 ページ）	（オプション）クラスタ内の最初のパブリッシャ ノードだけを復元する場合は、この手順を使用します。
Step 2	後続クラスタ ノードの復元（416ページ）	（オプション）クラスタ内のサブスクライバ ノードを復元する場合は、この手順を使用します。
Step 3	パブリッシャの再構築後の1回のステップでのクラスタの復元 （418 ページ）	（オプション）パブリッシャがすでに再構築されている場合、1回のステップでクラスタ全体を復元するには、次の手順に従ってください。
Step 4	クラスタ全体の復元 （420 ページ）	（オプション）パブリッシャ ノードを含む、クラスタ内のすべてのノードを復元するには、この手順を使用します。主要な

	コマンドまたはアクション	目的
		ハードドライブで障害またはアップグレードが発生した場合や、ハード ドライブを移行する場合には、クラスタ内のすべてのノードの再構築が必要になる場合があります。
Step 5	前回正常起動時の設定へのノードまたはクラスタの復元 （421 ページ）	（オプション）前回正常起動時の設定にノードを復元する場合に限り、この手順を使用します。ハード ドライブ障害やその他のハードウェア障害の後には使用しないでください。
Step 6	ノードの再起動 （422 ページ）	ノードを再起動するには、この手順を使用します。
Step 7	復元ジョブ ステータスのチェック （423 ページ）	（オプション）復元ジョブ ステータスを確認するには、この手順を使用します。
Step 8	復元履歴の表示 （423 ページ）	（オプション）復元履歴を表示するには、この手順を使用します。

最初のノードのみの復元

再構築後に最初のノードを復元する場合は、バックアップ デバイスを設定する必要があります。

この手順は、Cisco Unified Communications Manager の最初のノード（パブリッシャ ノードとも呼ばれます）に対して実行できます。その他の Cisco Unified Communications Manager ノードおよびすべての IM and Presence サービス ノードは、セカンダリ ノードまたはサブスクライバと見なされます。

始める前に

クラスタ内に IM and Presence サービス ノードがある場合は、最初のノードを復元するときに、ノードが実行されており、アクセス可能であることを確認してください。これは、この手順の実行中に有効なバックアップ ファイルを見つけるために必須です。

手順

Step 1 ディザスタ リカバリ システムから、**[復元（Restore）] > [復元ウィザード（Restore Wizard）]** を選択します。

Step 2 [復元ウィザード ステップ 1（Restore Wizard Step 1）] ウィンドウの [バックアップ デバイスの選択（Select Backup Device）] 領域で、復元する適切なバックアップ デバイスを選択します。

Step 3 [次へ（Next）] をクリックします。

Step 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）] ウィンドウで、復元するバックアップ ファイルを選択します。

（注） バックアップファイル名から、バックアップファイルが作成された日付と時刻がわかります。

Step 5 [次へ（Next）] をクリックします。

Step 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）] ウィンドウで、[次へ（Next）] をクリックします。

Step 7 復元する機能を選択します。

（注） バックアップ対象として選択した機能が表示されます。

Step 8 [次へ（Next）] をクリックします。[復元ウィザード ステップ 4（Restore Wizard Step 4）] ウィンドウが表示されます。

Step 9 ファイル整合性チェックを実行する場合は、[SHA1 メッセージダイジェストを使用してファイル整合性チェックを実行する（Select the Perform file integrity check using SHA1 Message Digest）] チェックボックスをオンにします。

（注） ファイル整合性チェックは任意で、SFTP バックアップの場合にだけ必要です。

ファイル整合性チェックの処理はCPUおよびネットワーク帯域幅を大量に消費するため、復元プロセスの処理速度が低下します。

FIPS モードでのメッセージダイジェスト検証にも SHA-1 を使用できます。SHA-1 は、デジタル署名に使用されないHMACやランダムビット生成などのハッシュ関数アプリケーションでのすべての非デジタル署名の使用に許可されています。たとえば、SHA-1 は引き続きチェックサムの計算に使用できます。署名の生成と検証にのみ、SHA-1 は使用できません。

Step 10 復元するノードを選択します。

Step 11 [復元（Restore）] をクリックして、データを復元します。

Step 12 [次へ（Next）] をクリックします。

Step 13 復元するノードの選択を求められたら、最初のノード（パブリッシャ）だけを選択します。

注意 このときに後続（サブスクライバ）ノードは選択しないでください。復元を試みても失敗します。

Step 14 （オプション）[サーバ名の選択（Select Server Name）] ドロップダウン リストから、パブリッシャ データベース復元元のサブスクライバ ノードを選択します。選択したサブスクライバ ノードが稼働しており、クラスタに接続されていることを確認してください。
ディザスタ リカバリ システムでバックアップ ファイルのすべてのデータベース以外の情報が復元され、選択した後続ノードから最新のデータベースが取り出されます。

（注） このオプションは、選択したバックアップ ファイルに CCMDB データベース コンポーネントが含まれている場合にのみ表示されます。まず、パブリッシャ ノードだけが完全に復元されますが、ステップ 14 を実行し、後続のクラスタ ノードを再起動すると、ディザスタ リカバリ システムはデータベース レプリケーションを実行し、完全にすべてのクラスタ ノードのデータベースが同期されます。これにより、すべてのクラスタ ノードに最新のデータを使用していることが保障されます。

Step 15 [復元（Restore）] をクリックします。

Step 16 パブリッシャ ノードにデータが復元されます。復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

（注） 最初のノードを復元すると、Cisco Unified Communications Manager データベース全体がクラスタに復元されます。そのため、復元しているノードの数とデータベースのサイズによっては、数時間かかることがあります。復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

Step 17 [復元ステータス（Restore Status）] ウィンドウの [完了率（Percentage Complete）] フィールドに 100% と表示されたら、サーバを再起動します。クラスタ内のすべてのノードの再起動は最初のノードのみへの復元の場合に必要となります。後続ノードを再起動する前に、必ず最初のノードを再起動してください。サーバの再起動方法については、「次の作業」の項を参照してください。

（注） Cisco Unified Communications Manager ノードだけを復元する場合は、Cisco Unified Communications Manager and IM and Presence Service サービス クラスタを再起動する必要があります。

IM and Presence サービスのパブリッシャ ノードのみを復元する場合は、IM and Presence サービス クラスタを再起動する必要があります。

次のタスク

- （オプション）復元のステータスを表示するには、次を参照してください。 復元ジョブ ステータスのチェック （423 ページ）
- ノードを再起動するには、次を参照してください： ノードの再起動 （422 ページ）

後続クラスタ ノードの復元

この手順は、Cisco Unified Communications Manager のサブスクライバ（後続）ノードにのみ適用されます。インストールされる最初の Cisco Unified Communications Manager ノードはパブリッシャ ノードです。その他すべての Cisco Unified Communications Manager ノードおよびすべての IM and Presence サービス ノードはサブスクライバ ノードです。

クラスタ内の 1 つ以上の Cisco Unified Communications Manager サブスクライバ ノードを復元するには、次の手順に従います。

始める前に

復元操作を実行する場合は事前に、復元のホスト名、IP アドレス、DNS 設定、および配置タイプが、復元するバックアップ ファイルのホスト名、IP アドレス、DNS 設定、および配置タイプに一致することを確認します。ディザスタ リカバリ システムでは、ホスト名、IP アドレス、DNS 設定、および配置タイプが異なると復元が行われません。

サーバにインストールされているソフトウェアのバージョンが復元するバックアップ ファイルのバージョンに一致することを確認します。ディザスタ リカバリ システムは、一致するソフトウェア バージョンのみを復元操作でサポートします。再構築後に後続ノードを復元している場合は、バックアップ デバイスを設定する必要があります。

手順

Step 1 ディザスタ リカバリ システムから、**[復元（Restore）] > [復元ウィザード（Restore Wizard）]** を選択します。

Step 2 [復元ウィザード ステップ 1（Restore Wizard Step 1）] ウィンドウの [バックアップ デバイスの選択（Select Backup Device）] 領域で、復元元のバックアップ デバイスを選択します。

Step 3 [次へ（Next）] をクリックします。

Step 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）] ウィンドウで、復元するバックアップ ファイルを選択します。

Step 5 [次へ（Next）] をクリックします。

Step 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）] ウィンドウで、復元する機能を選択します。

（注） 選択したファイルにバックアップされた機能だけが表示されます。

Step 7 [次へ（Next）] をクリックします。[復元ウィザード ステップ 4（Restore Wizard Step 4）] ウィンドウが表示されます。

Step 8 [復元ウィザード ステップ 4（Restore Wizard Step 4）] ウィンドウで、復元するノードを選択するよう求められたら、後続ノードのみを選択します。

Step 9 [復元（Restore）] をクリックします。

Step 10 後続ノードにデータが復元されます。復元ステータスの確認方法については、「次の作業」の項を参照してください。

（注） 復元プロセス中、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] または [ユーザ オプション（User Options）] に関するタスクを実行しないでください。

Step 11 [復元ステータス（Restore Status）] ウィンドウの [完了率（Percentage Complete）] フィールドに 100% と表示されたら、復元した 2 次サーバを再起動します。クラスタ内のすべてのノードの再起動は最初のノードのみへの復元の場合に必要となります。後続ノードを再起動する前に、必ず最初のノードを再起動してください。サーバの再起動方法については、「次の作業」の項を参照してください。

（注） 最初の IM and Presence サービス ノードが復元されたら、後続の IM and Presence Service ノードを再起動する前に、必ず最初の IM and Presence Service ノードを再起動してください。

次のタスク

- （オプション）復元のステータスを表示するには、次を参照してください。 復元ジョブ ステータスのチェック （423 ページ）
- ノードを再起動するには、次を参照してください： ノードの再起動 （422 ページ）

パブリッシャの再構築後の 1 回のステップでのクラスタの復元

復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。パブリッシャがすでに再構築されている場合、または新しくインストールされた場合に、1 回のステップでクラスタ全体を復元する場合は、次の手順に従います。

手順

Step 1 ディザスタ リカバリ システムから、**[復元（Restore）] > [復元ウィザード（Restore Wizard）]** を選択します。

Step 2 [復元ウィザード ステップ 1（Restore Wizard Step 1）] ウィンドウの [バックアップ デバイスの選択（Select Backup Device）] 領域で、復元するバックアップ デバイスを選択します。

Step 3 [次へ（Next）] をクリックします。

Step 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）] ウィンドウで、復元するバックアップ ファイルを選択します。

バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。

クラスタ全体を復元するクラスタのバックアップ ファイルだけを選択します。

Step 5 [次へ（Next）] をクリックします。

Step 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）] ウィンドウで、復元する機能を選択します。

画面には、復元する機能のうち、バックアップ ファイルに保存された機能のみが表示されます。

Step 7 [次へ（Next）] をクリックします。

Step 8 [復元ウィザード ステップ 4（Restore Wizard Step 4）] ウィンドウで、[1 ステップでの復元（One-Step Restore）] をクリックします。

このオプションは、復元対象として選択されたバックアップ ファイルがクラスタのバックアップ ファイルであり、復元対象として選択された機能に、パブリッシャとサブスクライバの両方のノードに登録された機能が含まれている場合にのみ、[復元ウィザード ステップ 4（Restore Wizard Step

4）] ウィンドウに表示されます。詳細については、最初のノードのみの復元（414 ページ）および後続クラスタ ノードの復元（416 ページ）を参照してください。

（注） パブリッシャがクラスタ対応になりませんでした。1 ステップでの復元を開始できません（Publisher has failed to become cluster aware. Cannot start one-step restore）」というステータス メッセージが表示されたら、パブリッシャ ノードを復元してからサブスクライバ ノードを復元する必要があります。詳細については、「関連項目」を参照してください。

このオプションでは、パブリッシャがクラスタ対応になり、そのためには 5 分かかります。このオプションをクリックすると、ステータス メッセージに「「パブリッシャがクラスタ対応になるまで 5 分間待機してください。この期間にバックアップまたは復元処理を開始しないでください。（Please wait for 5 minutes until Publisher becomes cluster aware and do not start any backup or restore activity in this time period.）」」と表示されます。

この待ち時間の経過後に、パブリッシャがクラスタ対応になると、「「パブリッシャがクラスタ対応になりました」が表示されます。サーバを選択し、[復元（Restore）] をクリックしてクラスタ全体の復元を開始してください。（Please select the servers and click on Restore to start the restore of entire cluster）」」というステータス メッセージが表示されます。

この待ち時間の経過後、パブリッシャがクラスタ対応にならない場合、「パブリッシャがクラスタ対応にならなかったため、1 ステップでの復元を開始できません。通常の 2 ステップでの復元を実行してください。（Publisher has failed to become cluster aware. Cannot start one-step restore. Please go ahead and do a normal two-step restore.）」というステータス メッセージが表示されます。クラスタ全体を 2 ステップ（パブリッシャとサブスクライバ）で復元するには、最初のノードのみの復元（414 ページ）と 後続クラスタ ノードの復元（416 ページ）で説明する手順を実行してください。

Step 9 復元するノードの選択を求められたら、クラスタ内のすべてのノードを選択します。

最初のノードを復元すると、ディザスタ リカバリ システムが自動的に後続ノードに Cisco Unified Communications Manager データベース（CCMDB）を復元します。そのため、復元しているノードの数とデータベースのサイズによっては、数時間かかることがあります。

Step 10 [復元（Restore）] をクリックします。
クラスタ内のすべてのノードでデータが復元されます。

Step 11 [復元ステータス（Restore Status）] ウィンドウの [完了率（Percentage Complete）] フィールドに 100% と表示されたら、サーバを再起動します。クラスタ内のすべてのノードの再起動は最初のノードのみへの復元の場合に必要となります。後続ノードを再起動する前に、必ず最初のノードを再起動してください。サーバの再起動方法については、「次の作業」の項を参照してください。

次のタスク

- （オプション）復元のステータスを表示するには、次を参照してください。復元ジョブ ステータスのチェック（423 ページ）

- ノードを再起動するには、次を参照してください： ノードの再起動（422 ページ）

クラスタ全体の復元

主要なハードドライブで障害またはアップグレードが発生した場合や、ハードドライブを移行する場合には、クラスタ内のすべてのノードの再構築が必要です。クラスタ全体を復元するには、次の手順を実行します。

ネットワーク カードの交換やメモリの増設など他のほとんどのハードウェア アップグレードでは、次の手順を実行する必要はありません。

手順

Step 1 ディザスタ リカバリ システムから、**[復元（Restore）]** > **[復元ウィザード（Restore Wizard）]** を選択します。

Step 2 [バックアップ デバイスの選択（Select Backup Device）] エリアで、復元する適切なバックアップ デバイスを選択します。

Step 3 [次へ（Next）] をクリックします。

Step 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）] ウィンドウで、復元するバックアップ ファイルを選択します。

（注） バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。

Step 5 [次へ（Next）] をクリックします。

Step 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）] ウィンドウで、[次へ（Next）] をクリックします。

Step 7 [復元ウィザード ステップ 4（Restore Wizard Step 4）] ウィンドウで復元ノードの選択を求められたら、すべてのノードを選択します。

Step 8 [復元（Restore）] をクリックして、データを復元します。

最初のノードを復元すると、ディザスタ リカバリ システムが自動的に後続ノードに Cisco Unified Communications Manager データベース（CCMDB）を復元します。そのため、ノードの数とデータベースのサイズによっては、最大数時間かかることがあります。

すべてのノードでデータが復元されます。

（注） 復元プロセス中、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] または [ユーザ オプション（User Options）] に関するタスクを実行しないでください。

復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

Step 9 復元プロセスが完了したら、サーバを再起動します。サーバの再起動方法の詳細については、「次の作業」セクションを参照してください。

（注） 必ず最初のノードを再起動してから、後続ノードを再起動してください。

最初のノードが再起動し、Cisco Unified Communications Manager の復元後のバージョンが実行されたら、後続ノードを再起動します。

Step 10 レプリケーションはクラスタのリブート後に自動的にセットアップされます。『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の説明に従って「utils dbreplication runtimestate」 CLI コマンドを使用して、すべてのノードで [レプリケーション ステータス（Replication Status）] の値を確認します。各ノードの値は 2 になっているはずです。

（注） クラスタのサイズによっては、後続ノードの再起動後に、後続ノードでのデータベース レプリケーションが完了するまでに時間がかかる場合があります。

ヒント レプリケーションが正しくセットアップされない場合は、『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』の説明に従って「utils dbreplication rebuild」CLI コマンドを使用します。

次のタスク

- （オプション）復元のステータスを表示するには、次を参照してください。 復元ジョブ ステータスのチェック （423 ページ）
- ノードを再起動するには、次を参照してください： ノードの再起動 （422 ページ）

前回正常起動時の設定へのノードまたはクラスタの復元

前回正常起動時の設定にノードまたはクラスタを復元するには、次の手順に従います。

始める前に

- 復元ファイルに、バックアップ ファイルで設定されているホスト名、IP アドレス、DNS 設定、および配置タイプが含まれていることを確認します。
- サーバにインストールされている Cisco Unified Communications Manager のバージョンが復元するバックアップ ファイルのバージョンに一致することを確認します。
- この手順は、前回正常起動時の設定にノードを復元する場合にのみ使用してください。

手順

Step 1 ディザスタ リカバリ システムから、**[復元（Restore）] > [復元ウィザード（Restore Wizard）]** を選択します。

Step 2 [バックアップ デバイスの選択（Select Backup Device）] 領域で、復元する適切なバックアップ デバイスを選択します。

Step 3 [次へ（Next）] をクリックします。

Step 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）] ウィンドウで、復元するバックアップ ファイルを選択します。

（注） バックアップファイル名から、バックアップファイルが作成された日付と時刻がわかります。

Step 5 [次へ（Next）] をクリックします。

Step 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）] ウィンドウで、[次へ（Next）] をクリックします。

Step 7 復元ノードを選択するように求められたら、該当するノードを選択します。
選択したノードにデータが復元されます。

Step 8 クラスタ内のすべてのノードを再起動します。後続の Cisco Unified Communications Manager ノードを再起動する前に、最初の Cisco Unified Communications Manager ノードを再起動します。クラスタに Cisco IM and Presence ノードもある場合は、最初の Cisco IM and Presence ノードを再起動してから、後続の IM and Presence ノードを再起動します。詳細については、「次の作業」の項を参照してください。

ノードの再起動

データを復元したら、ノードを再起動する必要があります。

パブリッシャ ノード（最初のノード）を復元したら、最初にパブリッシャ ノードを再起動する必要があります。サブスクライバ ノードは必ず、パブリッシャ ノードが再起動し、ソフトウェアの復元されたバージョンを正常に実行し始めた後で再起動してください。

（注） CUCM パブリッシャノードがオフラインの場合は、IM and Presence サブスクライバノードを再起動しないでください。このような場合、サブスクライバノードがCUCMパブリッシャに接続できないため、ノードサービスが起動しません。

注意 この手順を実行すると、システムが再起動し、一時的に使用できない状態になります。

再起動する必要があるクラスタ内のすべてのノードでこの手順を実行します。

手順

Step 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] から、**[設定（Settings）] > [バージョン（Version）]** を選択します。

Step 2 ノードを再起動するには、[再起動（Restart）] をクリックします。

Step 3 レプリケーションはクラスタのリブート後に自動的に設定されます。**utils dbreplication runtimestate** CLI コマンドを使用して、すべてのノードで [レプリケーション ステータス（Replication Status）] 値を確認します。各ノードの値は 2 になっているはずです。CLI コマンドの詳細については、『Cisco Unified Communications (CallManager) Command References』を参照してください。

レプリケーションが正しくセットアップされない場合は、『*Command Line Reference Guide for Cisco Unified Communications Solutions*』の説明に従って **utils dbreplication reset** CLI コマンドを使用します。

（注） クラスタのサイズによっては、後続ノードの再起動後に、後続ノードでのデータベース レプリケーションが完了するまでに数時間かかる場合があります。

次のタスク

（オプション）復元のステータスを表示するには、復元ジョブ ステータスのチェック （423 ページ）を参照してください。

復元ジョブ ステータスのチェック

次の手順に従って、復元ジョブ ステータスをチェックします。

手順

Step 1 ディザスタ リカバリ システムで、**[復元（Restore）] > [現在のステータス（Current Status）]** を選択します。

Step 2 [復元ステータス（Restore Status）] ウィンドウで、ログ ファイル名のリンクをクリックし、復元ステータスを表示します。

復元履歴の表示

復元履歴を参照するには、次の手順を実行します。

手順

Step 1 [Disaster Recovery System] で、**[復元（Restore）]** > **[履歴（History）]** を選択します。

Step 2 [復元履歴（Restore History）] ウィンドウで、ファイル名、バックアップ デバイス、完了日、結果、バージョン、復元された機能、失敗した機能など、実行した復元を表示できます。

[復元履歴（Restore History）] ウィンドウには、最新の 20 個の復元ジョブだけが表示されます。

データ認証

トレース ファイル

トラブルシューティングを行う際、またはログの収集中には、トレース ファイルの保存先として次の場所が使用されます。

マスターエージェント、GUI、各ローカルエージェント、およびJSchライブラリのトレースファイルは次の場所に書き込まれます。

- マスター エージェントの場合、トレース ファイルは platform/drf/trace/drfMA0* にあります。
- 各ローカル エージェントの場合、トレース ファイルは platform/drf/trace/drfLA0* にあります。
- GUI の場合、トレース ファイルは platform/drf/trace/drfConfLib0* にあります。
- JSch の場合、トレース ファイルは platform/drf/trace/drfJSch* にあります。

詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html）を参照してください。

コマンドライン インターフェイス

ディザスタ リカバリ システムでは、次の表に示すように、バックアップおよび復元機能のサブセットにコマンドラインからアクセスできます。これらのコマンドの内容とコマンドライン インターフェイスの使用方法の詳細については、『*Command Line Interface（CLI）Reference Guide for Cisco Unified Presence*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html）を参照してください。

表 *44 :* ディザスタ リカバリ システムのコマンドライン インターフェイス

コマンド	説明
utils disaster_recovery estimate_tar_size	SFTP/Local デバイスからのバックアップ tar の概算サイズを表示し、機能リストのパラメータを 1 つ要求します。
utils disaster_recovery backup	ディザスタ リカバリ システムのインターフェイスに設定されている機能を使用して、手動バックアップを開始します。
utils disaster_recovery jschLogs	JSch ライブラリのロギングを有効または無効にします。
utils disaster_recovery restore	復元を開始します。復元するバックアップ場所、ファイル名、機能、およびノードを指定するためのパラメータが必要です。
utils disaster_recovery status	進行中のバックアップ ジョブまたは復元ジョブのステータスを表示します。
utils disaster_recovery show_backupfiles	既存のバックアップ ファイルを表示します。
utils disaster_recovery cancel_backup	進行中のバックアップ ジョブをキャンセルします。
utils disaster_recovery show_registration	現在設定されている登録を表示します。
utils disaster_recovery device add	ネットワーク デバイスを追加します。
utils disaster_recovery device delete	デバイスを削除します。
utils disaster_recovery device list	すべてのデバイスを一覧表示します。
utils disaster_recovery schedule add	スケジュールを追加します。
utils disaster_recovery schedule delete	スケジュールを削除します。
utils disaster_recovery schedule disable	スケジュールを無効にします。
utils disaster_recovery schedule enable	スケジュールを有効にします。
utils disaster_recovery schedule list	すべてのスケジュールを一覧表示します。
utils disaster_recovery backup	ディザスタ リカバリ システムのインターフェイスに設定されている機能を使用して、手動バックアップを開始します。

コマンド	説明
utils disaster_recovery restore	復元を開始します。復元するバックアップ場所、ファイル名、機能、およびノードを指定するためのパラメータが必要です。
utils disaster_recovery status	進行中のバックアップ ジョブまたは復元ジョブのステータスを表示します。
utils disaster_recovery show_backupfiles	既存のバックアップ ファイルを表示します。
utils disaster_recovery cancel_backup	進行中のバックアップ ジョブをキャンセルします。
utils disaster_recovery show_registration	現在設定されている登録を表示します。

アラームおよびメッセージ

アラームおよびメッセージ

ディザスタ リカバリ システムは、バックアップまたは復元手順の実行時に発生するさまざまなエラーのアラームを発行します。次の表に、ディザスタ リカバリ システムのアラームの一覧を記載します。

表 *45*: ディザスタ リカバリ システムのアラームとメッセージ

アラーム名	説明	説明
DRFBackupDeviceError	DRF バックアップ プロセスでデバイスへのアクセスに関する問題が発生しています。	DRS バックアップ プロセスでスへのアクセス中にエラーがした。
DRFBackupFailure	シスコ DRF バックアップ プロセスが失敗しました。	DRS バックアップ プロセスでが発生しました。
DRFBackupInProgress	別のバックアップの実行中は、新規バックアップを開始できません。	DRSは、別のバックアップの新規バックアップを開始でき
DRFInternalProcessFailure	DRF 内部プロセスでエラーが発生しました。	DRS内部プロセスでエラーがした。
DRFLA2MAFailure	DRF ローカル エージェントが、マスターエージェントに接続できません。	DRS ローカル エージェントがターエージェントに接続でき
DRFLocalAgentStartFailure	DRF ローカル エージェントが開始されません。	DRS ローカル エージェントがしている可能性があります。

アラーム名	説明	説明
DRFMA2LAFailure	DRF マスター エージェントがローカル エージェントに接続しません。	DRS マスター エージェンル エージェントに接続で
DRFMABackupComponentFailure	DRF は、少なくとも 1 つのコンポーネントをバックアップできません。	DRS は、コンポーネントバックアップするように要が、バックアッププロセスが発生し、コンポーネントアップされませんでした。
DRFMABackupNodeDisconnect	バックアップされるノードが、バックアップの完了前にマスターエージェントから切断されました。	DRS マスター エージェンUnified Communications Maでバックアップ操作を実行きに、そのノードはバックが完了する前に切断され
DRFMARestoreComponentFailure	DRF は、少なくとも 1 つのコンポーネントを復元できません。	DRS は、コンポーネントの元するように要求しましたロセス中にエラーが発生しネントは復元されませんで
DRFMARestoreNodeDisconnect	復元されるノードが、復元の完了前にマスターエージェントから切断されました。	DRS マスター エージェンUnified Communications Maで復元操作を実行しているのノードは復元操作が完了断されました。
DRFMasterAgentStartFailure	DRF マスター エージェントが開始されませんでした。	DRS マスター エージェンしている可能性があります
DRFNoRegisteredComponent	使用可能な登録済みコンポーネントがないため、バックアップが失敗しました。	使用可能な登録済みコンポないため、DRS バックアップました。
DRFNoRegisteredFeature	バックアップする機能が選択されませんでした。	バックアップする機能が選んでした。
DRFRestoreDeviceError	DRF 復元プロセスでデバイスへのアクセスに関する問題が発生しています。	DRS 復元プロセスは、デバみ取ることができません。
DRFRestoreFailure	DRF 復元プロセスが失敗しました。	DRS 復元プロセスでエラーした。
DRFSftpFailure	DRF SFTP 操作でエラーが発生しています。	DRS SFTP 操作でエラーがます。

アラーム名	説明	説明
DRFSecurityViolation	DRFシステムが、セキュリティ違反となる可能性がある悪意のあるパターンを検出しました。	DRF ネットワーク メッセージ コードインジェクションやデ リ トラバーサルなど、セキュ 反となる可能性がある悪意の ターンが含まれています。DR ワーク メッセージがブロック ます。
DRFTruststoreMissing	ノードで IPsec 信頼ストアが見つかりません。	ノードで IPsec 信頼ストアが ません。DRF ローカル エー が、マスターエージェントに ません。
DRFUnknownClient	パブリッシャのDRFマスターエージェントが、クラスタ外部の不明なサーバからクライアント接続要求を受け取りました。要求は拒否されました。	パブリッシャのDRFマスター ントが、クラスタ外部の不明 からクライアント接続要求を ました。要求は拒否されまし
DRFBackupCompleted	DRFバックアップが正常に完了しました。	DRFバックアップが正常に完 た。
DRFRestoreCompleted	DRF 復元が正常に完了しました。	DRF 復元が正常に完了しまし
DRFNoBackupTaken	現在のシステムの有効なバックアップが見つかりませんでした。	アップグレード/移行または新 トール後に、現在のシステム バックアップが見つかりませ た。
DRFComponentRegistered	DRFにより、要求されたコンポーネントが正常に登録されました。	DRFにより、要求されたコン トが正常に登録されました。
DRFRegistrationFailure	DRF 登録操作が失敗しました。	内部エラーが原因で、コンポ に対する DRF 登録操作が失 た。
DRFComponentDeRegistered	DRFは正常に要求されたコンポーネントの登録をキャンセルしました。	DRFは正常に要求されたコン トの登録をキャンセルしまし
DRFDeRegistrationFailure	コンポーネントの DRF 登録解除リクエストが失敗しました。	コンポーネントの DRF 登録解 エストが失敗しました。
DRFFailure	DRFバックアップまたは復元プロセスが失敗しました。	DRFバックアップまたは復元 でエラーが発生しました。
DRFRestoreInternalError	DRF復元オペレーションでエラーが発生しました。復元は内部的にキャンセルされました。	DRF復元オペレーションでエ 生しました。復元は内部的に ルされました。

アラーム名	説明	説明
DRFLogDirAccessFailure	DRF は、ログ ディレクトリにアクセスできませんでした。	DRF は、ログ ディレクトスできませんでした。
DRFDeRegisteredServer	DRF がサーバのすべてのコンポーネントを自動的に登録解除しました。	サーバーが Unified Commu Manager クラスタから切断可能性があります。
DRFSchedulerDisabled	設定された機能がバックアップで使用できないため、DRF スケジューラは無効になっています。	設定された機能がバックアできないため、DRF スケジ効になっています
DRFSchedulerUpdated	機能が登録解除されたため、DRF でスケジュールされたバックアップ設定が自動的に更新されます。	機能が登録解除されたため ケジュールされたバックア自動的に更新されます

復元の連携動作と制約事項

復元の制約事項

ディザスタ リカバリ システムを使用して Cisco Unified Communications Manager または IM and Presence Service を復元する場合、以下の制約事項が適用されます。

表 *46 :* 復元の制約事項

制限事項	説明
エクスポートの制限	制限されたバージョンの DRS バックアップは、制限されたバージョンにのみ復元できます。また、制限されていないバージョンのバックアップは、制限されていないバージョンにのみ復元できます。Cisco Unified Communications Manager の米国輸出無制限バージョンにアップグレードした場合、その後、このソフトウェアの米国輸出制限バージョンへのアップグレード、または新規インストールを実行できなくなります。
プラットフォームの移行	ディザスタ リカバリ システムを使用してプラットフォーム間で（たとえば、Windows から Linux へ、または Linux から Windows へ）データを移行することはできません。復元は、バックアップと同じ製品バージョンで実行する必要があります。Windows ベースのプラットフォームから Linux ベースのプラットフォームへのデータ移行については、『*Data Migration Assistant User Guide*』を参照してください。

制限事項	説明
HW の交換と移行	DRS復元を実行してデータを新しいサーバに移行する場合、新しいサーバに古いサーバーが使用していたのと同じ IP アドレスとホスト名を割り当てる必要があります。さらに、バックアップの取得時に DNS が設定されている場合、復元を実行する前に、同じ DNS 設定がある必要があります。 サーバの交換の詳細については、『*Replacing a Single Server or Cluster for Cisco Unified Communications Manager*』ガイドを参照してください。 また、ハードウェアの交換後は、証明書信頼リスト（CTL）クライアントを実行する必要もあります。後続ノード（サブスクライバ）サーバを復元しない場合には、CTL クライアントを実行する必要があります。他の場合、DRS は必要な証明書をバックアップします。詳細については、『*Cisco Unified Communications Manager Security Guide*』の「「Installing the CTL Client」」と「「Configuring the CTL Client 」」の手順を参照してください。
クラスタ間のエクステンション モビリティ（Extension Mobility Cross Cluster）	バックアップ時にリモートクラスタにログインしていた Extension Mobility Cross Cluster ユーザは、復元後もログインしたままとなります。

（注） DRS バックアップ/復元は CPU 指向の高いプロセスです。バックアップと復元の対象となるコンポーネントの 1 つに、Smart License Manager があります。このプロセス中に、Smart License Manager サービスが再起動します。高いリソース使用率が予想されるため、メンテナンス期間中にプロセスをスケジュールすることをお勧めします。

Cisco Unified Communications サーバ コンポーネントの復元が正常に完了した後、Cisco Unified Communications Manager を Cisco Smart Software Manager または Cisco スマート ソフトウェア マネージャ サテライトに登録してください。バックアップを作成する前に製品がすでに登録されていたとしても、その製品を再登録してライセンス情報を更新する必要があります。

Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに製品を登録する方法の詳細については、ご使用のリリースの『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

トラブルシューティング

より小さい仮想マシンへの DRS 復元の失敗

問題

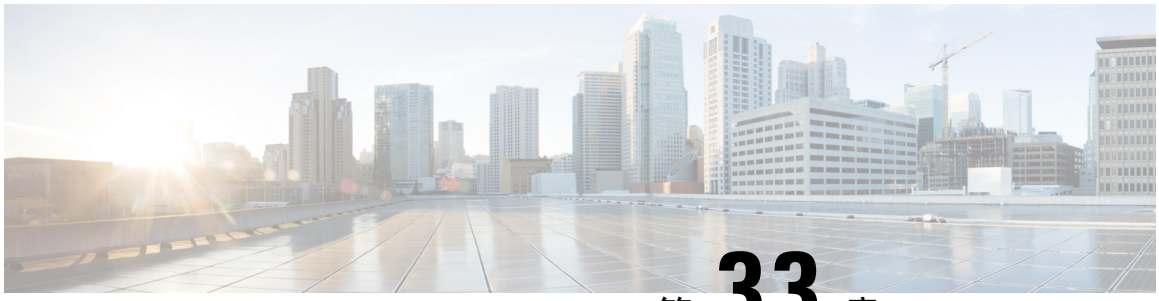
IM and Presence サービス ノードをディスク容量がより小さい VM に復元すると、データベースの復元が失敗することがあります。

原因

大きいディスク サイズから小さいディスク サイズに移行したときに、この障害が発生します。

解決策

2 個の仮想ディスクがある OVA テンプレートから、復元用の VM を展開します。



第 33 章

連絡先リストの一括管理

一括管理の概要

IM and Presence サービス一括管理ツールを使用すると、多数の IM and Presence サービス ユーザに対して、以下の一括処理を実行することができます。

- Microsoft 移行プロセスで使用するために、ユーザの連絡先 ID 名を変更します。
- 特定のノードまたはプレゼンス冗長グループに属するユーザの連絡先リストおよび非プレゼンスの連絡先リストを CSV データファイルにエクスポートします。

（注） 非プレゼンス連絡先は、IM アドレスを持たない連絡先であり、この手順でのみエクスポートできます。

- エクスポートしたユーザ連絡先リスト、非プレゼンス連絡先リスト、およびユーザロケーション移行の詳細を別のクラスタの別のノードまたはプレゼンス冗長グループにインポートすることもできます。新規ユーザーの連絡先リストを事前入力するか、既存の連絡先リストに追加します。
- この機能によって、クラスタ間のユーザの移行が容易になります。

一括管理の要件

ユーザ連絡先リストをインポートする前に：

1. Cisco Unified Communications Manager でユーザをプロビジョニングします。

2. Cisco Unified Communications Manager でユーザに IM and Presence Service のライセンスが供与されていることを確認します。

（注） デフォルトの連絡先リストのインポート速度は、仮想マシン展開のハードウェアのタイプに基づいています。**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）]>[システム（System）]>[サービス パラメータ（Service Parameters）]>[Cisco Bulk Provisioning Service]** を選択して、連絡先リストのインポート レートを変更できます。ただし、デフォルトのインポート レートを大きくすると、IM and Presence Service で CPU 使用率とメモリ使用率が高くなります。

一括管理タスク フロー

手順

	コマンドまたはアクション	目的
Step 1	ユーザ連絡先 ID の一括名前変更（435 ページ）	CSV ファイルをアップロードして、ユーザのリストの連絡先 ID 名を変更します。
Step 2	ユーザ連絡先リストと非プレゼンス連絡先リストの一括エクスポート（436 ページ）	ユーザの連絡先リストを CSV ファイルにエクスポートするには、以下の手順を実行します。その後、一括管理を使用して、ユーザの連絡先リストを別のノードまたはクラスタに移動することができます。
Step 3	ユーザの場所の詳細を一括エクスポート（437 ページ）	この手順を使用して、ユーザの場所の詳細を CSV ファイルにエクスポートします。その後、一括管理を使用して、ユーザの場所の詳細を別のノードまたはクラスタに移動することができます。
Step 4	以下の手順を実行して、ユーザ連絡先リストを IM and Presence Service にインポートします。 • 連絡先リストの最大サイズの確認（441 ページ） • 入力ファイルのアップロード（441 ページ） • 新しい一括管理ジョブの作成（447 ページ） • 一括管理ジョブの結果の確認（448 ページ）	

ユーザ連絡先 ID の一括名前変更

注意　連絡先 ID の一括名前変更は、Microsoft Server（たとえば Lync）から IM and Presence サービス サービスへのユーザの移行で使用されます。このツールのユーザ移行プロセスの一部としての使用方法についての詳しい手順については、Cisco.com の『Partitioned Intradomain Federation ガイド』を参照してください。それ以外の状況での、このツールの使用はサポートされません。

CSV ファイルをアップロードして、ユーザのリストの連絡先 ID 名を変更します。

手順

Step 1　すべての連絡先リスト内で名前を変更するコンタクト ID のリストを含んだ CSV ファイルをアップロードします。

a) {1}IM and Presence Service{1} のパブリッシャ ノードに移動します。
b) **Cisco Unified CM IM and Presence 管理**で、**一括管理 > ファイルのアップロード/ダウンロード**を選択します。。
c) **[新規追加]** をクリックします。
d) **[参照（Browse）]** をクリックして CSV ファイルを見つけて選択します。入力ファイルの詳細については、ユーザ連絡先 ID の一括変更ファイルの詳細（436 ページ）を参照してください。
e) ターゲットとして [連絡先（Contacts）] を選択します。
f) トランザクション タイプとして [連絡先の名前変更 - カスタム ファイル（Rename Contacts – Custom File）] を選択します。
g) **[Save（保存）]** を選択してファイルをアップロードします。

Step 2　パブリッシャ ノードで、**Cisco Unified CM IM and Presence 管理一括管理 > 連絡先リスト > 連絡先の名前の変更**を選択します。

Step 3　[ファイル名（File Name）] フィールドで、アップロードしたファイルを選択します。

Step 4　次のいずれかのアクションを選択します。

- 一括管理ジョブをただちに実行するには、[今すぐ実行（Run Immediately）] をクリックします。
- 一括管理ジョブを実行する時間をスケジュールするには、[後で実行（Run Later）] をクリックします。一括管理ツールのスケジューリング ジョブの詳細については、Cisco Unified CM IM and Presence Administration のオンライン ヘルプを参照してください。

Step 5　[送信（Submit）] をクリックします。

ジョブをただちに実行するように選択した場合は、[送信（Submit）] をクリックするとジョブが実行されます。

次のタスク

ユーザ連絡先リストと非プレゼンス連絡先リストの一括エクスポート（436 ページ）

ユーザ連絡先 ID の一括変更ファイルの詳細

このジョブを実行する前にアップロードするファイルは、以下の形式のCSVファイルである必要があります。

<Contact ID>, <New Contact ID>

<Contact ID> が、既存の連絡先 ID であり、<New Contact ID> が連絡先 ID の新しい形式です。

プレゼンス トポロジのユーザ割り当てウィンドウで表示される <Contact ID> がユーザの IM アドレスです。

次に、1 つのエントリを持つ CSV ファイルのサンプルを示します。

```
Contact ID, New Contact ID
john.smith@example.com, jsmith@example.com
```

ユーザ連絡先リストと非プレゼンス連絡先リストの一括エクスポート

ユーザの連絡先リストをCSVファイルにエクスポートするには、以下の手順を実行します。その後、一括管理を使用して、ユーザの連絡先リストを別のノードまたはクラスタに移動することができます。

- 連絡先リスト：このリストは、IM and Presence 連絡先で構成されます。IM アドレスがない連絡先は、エクスポートされません（非プレゼンス連絡先リストをエクスポートする必要があります）。
- 非プレゼンス連絡先リスト：このリストは、IMアドレスを持っていない連絡先で構成されます。

手順

Step 1 Cisco Unified CM IM and Presence 管理で、以下のいずれかを実行します。

- 連絡先リストをエクスポートするには、**一括管理**>**連絡先リスト**>**連絡先リストのエクスポート**を選択します。
- 非プレゼンス連絡先リストをエクスポートするには、**一括管理**>**非プレゼンス連絡先リスト**>**非プレゼンス連絡先リストのエクスポート** を選択し、次のステップはスキップします。

Step 2 連絡先リストのみ。連絡先リストをエクスポートするユーザを選択します。

a) **連絡先リストのオプションのエクスポート**の下で、連絡先リストのエクスポート先となるユーザのカテゴリを選択します。デフォルトでは、すべてのユーザの連絡先リストがエクスポートされます。

b) **検索** をクリックして、ユーザ リストを表示して、**次へ** をクリックします。

Step 3 [File Name（ファイル名）] フィールドに、CSV ファイルの名前を入力します。

Step 4 **ジョブ情報** の下で、このジョブをいつ実行するかを設定します。

- **すぐに実行**：連絡先のリストを即座にエクスポートするには、このボタンをオンにします。
- **後で実行**：ジョブを実行する時間をスケジュールする場合は、このボタンをオンにします。このオプションでは、**バルク管理** > **ジョブスケジューラ**の [ジョブスケジューラ] ページを使用して、このジョブが実行される時間をスケジュールする必要があります。

Step 5 [送信（Submit）] をクリックします。
すぐに実行する を選択した場合は、エクスポート ジョブは即座に実行されます。

Step 6 エクスポートファイルが作成された後の CSV ファイルのダウンロード：

a) Cisco Unified CM IM and Presence 管理で、**一括管理** > **ファイルのアップロード/ダウンロード**を選択します。
b) [**検索** をクリックしてエクスポート ファイルを選択します。
c) **選択したものをダウンロードする** をクリックして、アクセス可能なロケーションにファイルをダウンロードします。

ユーザの場所の詳細を一括エクスポート

この手順を使用して、ユーザの場所の詳細をCSVファイルにエクスポートします。その後、一括管理を使用して、ユーザの場所の詳細を別のノードまたはクラスタに移動することができます。

Procedure

Step 1 Cisco Unified CM IM and Presence の管理から、**[一括管理（Bulk Administration）] > [ユーザの場所の移行（User Location Migration）] > [ユーザの場所の詳細のエクスポート（Export User Location Details）]** を選択します。

Step 2 **[ユーザの場所の詳細を一括エクスポート（User Location Details Export）]** で、**[File Name（ファイル名）]** フィールドに、CSV ファイルの名前を入力します。

Step 3 **ジョブ情報** の下で、このジョブをいつ実行するかを設定します。

- **すぐに実行**—このボタンをオンにすると、ユーザの場所の詳細がすぐにエクスポートされます。
- **後で実行**：ジョブを実行する時間をスケジュールする場合は、このボタンをオンにします。このオプションでは、**[バルク管理（Bulk Administration）] > [ジョブスケジューラ（Job Scheduler）]** の **[ジョブスケジューラ（Job Scheduler）]** ページを使用して、このジョブが実行される時間をスケジュールする必要があります。

Step 4 [送信（Submit）] をクリックします。
[すぐに実行（Run Immediately）] を選択すると、エクスポートジョブがすぐに実行されます。

Step 5 エクスポートファイルが作成された後の CSV ファイルのダウンロード：

a) Cisco Unified CM IM and Presence 管理で、**[一括管理（Bulk Administration）] > [ファイルのアップロード/ダウンロード（Upload/Download Files）]**を選択します。
b) [**検索** をクリックしてエクスポート ファイルを選択します。

c) **選択したものをダウンロードする** をクリックして、アクセス可能なロケーションにファイルをダウンロードします。

エクスポート連絡先リストのファイルの詳細

次に、CSV ファイル エントリのサンプルを示します。

```
userA、example.com、userB、example.com、buddyB、General、0
```

BAT を使用すると、エクスポートする連絡先リストのユーザを検索して選択できます。ユーザ連絡先リストは次の形式の CSV ファイルにエクスポートされます。

```
<User ID>、<User Domain>、<Contact ID>、<Contact Domain>、<Nickname>、<Group Name>、<State>
```

次の表に、エクスポート ファイルのパラメータについて説明します。

パラメータ	説明
ユーザー ID	IM and Presence サービス ユーザのユーザ ID。 （注） この値は、ユーザの IM アドレスのユーザ部分です。
ユーザ ドメイン	IM and Presence サービス ユーザのプレゼンス ドメイン。 （注） この値は、ユーザの IM アドレスのドメイン部分です。 **例 1**：bjones@example.com （bjones はユーザ ID、example.com はユーザ ドメインです。） **例 2**： bjones @ usa @ example.com： bjones @ usa はユーザ ID であり、example.com は、ユーザのドメインです。
コンタクトID	連絡先リスト エントリのユーザ ID。
連絡先ドメイン（Contact Domain）	連絡先リストエントリのプレゼンス ドメイン。
ニックネーム	連絡先リスト エントリのニックネーム。 ユーザが連絡先のニックネームを指定しない場合、[ニックネーム（Nickname）] パラメータは空白です。

パラメータ	説明
グループ名	連絡先リストエントリが追加されるグループの名前。 ユーザの連絡先がグループに分けられていない場合、デフォルト グループ名が、[グループ名（Group Name）] フィールドに指定されます。
状態	名簿の状態は、名簿データベースに 10 進数形式で保存されます。

非プレゼンス連絡先リストのエクスポート ファイルの詳細

非プレゼンス ユーザ連絡先リストは次の形式の CSV ファイルにエクスポートされます。

```
<User JID>,<Contact JID>,<Group Name>,<Content Type>,<Version>,<Info>
```

次の表で、エクスポート ファイルのパラメータについて説明します。

パラメータ	説明
ユーザ JID	ユーザの JID。これは、ユーザの IM アドレスです。
コンタクト JID	連絡先リストエントリのユーザJID(使用可能な場合)。それ以外の場合は UUID です。
グループ名	連絡先リストエントリが追加されるグループの名前。
コンテンツ タイプ	情報フィールドで使用される textmime タイプおよびサブタイプ。
バージョン	[情報(info)] フィールドで使用されるコンテンツ タイプ。
情報	VCard 形式の連絡先リストエントリの連絡先情報。

次に、CSV ファイル エントリのサンプルを示します。

```
user2@cisco.com,ce463d44-02c3-4975-a37f-d4553e3f17e1,group01,text/directory,3,BEGIN:VCARD
ADR;TYPE=WORK:ADR\;WORK:\;\;123 Dublin rd\,\;Oranmore\;Galway\;\;Ireland
EMAIL;TYPE=X-CUSTOM1;X LABEL=Custom:testuser01@test.com N:test;user;;; NICKNAME:pizzaguy01
ORG:ABC TEL;TYPE=WORK,VOICE:5323534535 TITLE:QA VERSION:3.0 END:VCARD
```

ユーザの場所の詳細をエクスポートするためのファイルの詳細

ユーザの場所の詳細は次の形式の CSV ファイルにエクスポートされます。

```
<User JID>、<Access Type>、<Create Time>、<Item ID>、<Resource ID>、<Message Text>
```

Caution ファイル自体のサイズやユーザの場所情報が破損するリスクがあるため、エクスポートされた CSV ファイルを手動で変更しないことをお勧めします。

次の表で、エクスポート ファイルのパラメータについて説明します。

パラメータ	説明
ユーザ JID	ユーザの JID。これは、ユーザの IM アドレスです。
アクセスタイプ	アクセスタイプは、ユーザのアクセスタイプを定義します。 アクセスタイプの値は次のとおりです。 • W：ホワイトリスト • R：名簿グループ • O：オープン **Note** Jabber には「W」を使用します。
Create Time	[作成時間（Create Time）] には、アイテムが作成または更新された日時が表示されます。
アイテム ID	アイテム ID は、ユーザの特定のレコードを識別します。
リソースID	リソース ID は Jabber インスタンス ID です。
メッセージ テキスト	メッセージテキストは、ユーザの位置情報です。

次に、CSV ファイル エントリのサンプルを示します。

```
userA@example.com,W,2021-01-22
10:11:18.000001,7d0ec34c-458f-4fd2-9d15-58accac4af00,jabber_7151,

<geoloc
xmlns='http://jabber.org/protocol/geoloc'><description>newlocation104</description><street>104</street><mobile>0</mobile><enable>1</enable></geoloc>
```

ユーザ連絡先リストの一括インポート

連絡先リストの最大サイズの確認

IM and Presence Service での連絡先リストの最大サイズとウォッチャの最大設定を確認します。[Maximum Contact List Size（連絡先リストの最大サイズ）] のシステム デフォルト値は 200、[Maximum Watchers（ウォッチャの最大数）] のシステム デフォルト値は 200 です。

ユーザ連絡先リストのインポート中に連絡先リストの最大サイズと最大のウォッチャの設定を無制限に設定することを推奨します。BAT を使用して連絡先リストをインポートする際に最大連絡先リストサイズを超える場合でも、この手順により、移行された各ユーザー連絡先リストがデータを損失せずに完全にインポートされます。すべてのユーザを移行した後は、[Maximum Contact List Size（連絡先リストの最大サイズ）] と [Maximum Watchers（ウォッチャの最大数）] の設定値を必要な値にリセットできます。

連絡先をインポートするユーザを含むクラスタについてのみ、連絡先リストの最大サイズを確認する必要があります。プレゼンス設定を変更する場合、変更はクラスタ内のすべてのノードに適用されます。したがって、クラスタ内の IM and Presence データベース パブリッシャ ノードでのみこれらの設定を変更する必要があります。

次のタスク

入力ファイルのアップロード（441 ページ）

入力ファイルのアップロード

次の手順では、連絡先リストおよび非プレゼンス連絡先リストに BAT を使用して CSV 入力ファイルをアップロードする方法について説明します。

始める前に

連絡先リストの最大サイズの確認（441 ページ）

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**一括管理** > **ファイルのアップロード/ダウンロード**を選択します。

Step 2 **[新規追加]** をクリックします。

Step 3 **[参照（Browse）]** をクリックして CSV ファイルを見つけて選択します。

Step 4 対象設定：

- 連絡先リストの入力ファイルをアップロードする場合は、**連絡先リスト**を選択します。ユーザ連絡先リストの入力ファイルの詳細については、連絡先リストのファイル インポートの詳細（442 ページ）を参照してください。

- 非プレゼンス連絡先リストの入力ファイルをアップロードする場合は、**非プレゼンス連絡先リスト**を選択します。非プレゼンスユーザ連絡先リストの入力ファイルの詳細については、非プレゼンス連絡先リストのファイルインポートの詳細（445ページ）を参照してください。
- ユーザの場所の移行の詳細の入力ファイルをアップロードする場合は、**[ユーザの場所の移行（User Location Migration）]** を選択します。ユーザの場所の詳細入力ファイルの詳細については、「ユーザの場所の詳細をインポートするためのファイルの詳細（446ページ）」を参照してください。

Step 5 トランザクション タイプ：トランザクション タイプを選択します。

- 連絡先リストの入力ファイルをアップロードする場合は、**ユーザの連絡先 - カスタムファイルのインポート**を選択します。
- 非プレゼンス連絡先リストの入力ファイルをアップロードする場合は、**ユーザの非プレゼンス連絡先**を選択する
- ユーザの場所の移行の詳細の入力ファイルをアップロードする場合は、**[ユーザの場所の詳細のインポート（Import User Location Details）]** を選択します。

Step 6 [保存（Save）] をクリックし、ファイルをアップロードします。

次のタスク

新しい一括管理ジョブの作成（447 ページ）

連絡先リストのファイル インポートの詳細

入力ファイルは次の形式の CSV ファイルである必要があります。

```
<User ID>、<User Domain>、<Contact ID>、<Contact Domain>、<Nickname>、<Group Name>、<State>
```

次に、CSV ファイル エントリのサンプルを示します。

```
userA、example.com、userB、example.com、buddyB、General、0
```

次の表に、入力ファイルのパラメータについて説明します。

パラメータ	説明
ユーザー ID	これは必須パラメータです。 IM and Presence Service ユーザのユーザ ID。これには、最大 132 文字を使用できます。 （注） • この値は、ユーザの IM アドレスのユーザ部分です。 • 次の文字を含むユーザー ID の場合、JSMセッションは作成されません。 o a 2 ¼ ¾ - 3 µ 1 ½ ß ´ ← , – →

パラメータ	説明
ユーザ ドメイン	これは必須パラメータです。 IM and Presence Service ユーザのプレゼンス ドメイン。これには、最大 128 文字を使用できます。 （注） この値は、ユーザの IM アドレスのドメイン部分です。 **例 1**：bjones@example.com （bjones はユーザ ID、example.com はユーザ ドメインです。） **例 2**：bjones@usa@example.com （bjones@usa はユーザ ID、example.com はユーザ ドメインです。）
コンタクトID	これは必須パラメータです。 連絡先リストエントリのユーザ ID。これには、最大 132 文字を使用できます。
Contact Domain（連絡先ドメイン）	これは必須パラメータです。 連絡先リストエントリのプレゼンス ドメイン。次の制限は、ドメイン名の形式に適用されます。 • 長さは 128 文字以下である必要があります • 数字、大文字と小文字、およびハイフン（-）だけ含めます • ハイフン（-）で開始または終了してはいけません • ラベルの長さは 63 文字以下である必要があります • トップ レベル ドメインは文字だけで、少なくとも 2 文字にする必要があります
ニックネーム	連絡先リストエントリのニックネーム。これには、最大 255 文字を使用できます。

パラメータ	説明
グループ名	グループ名は必須パラメータです。 連絡先リストエントリが追加されるグループの名前。これには、最大 255 文字を使用できます。
状態	名簿の状態は、名簿データベースに 10 進数形式で保存されます。

非プレゼンス連絡先リストのファイル インポートの詳細

入力ファイルは次の形式の CSV ファイルである必要があります。

```
<User JID>,<Contact JID>,<Group Name>,<Content Type>,<Version>,<Info>
```

次に、CSV ファイル エントリのサンプルを示します。

```
user2@cisco.com,ce463d44-02c3-4975-a37f-d4553e3f17e1,group01,text/directory,3,BEGIN:VCARD
ADR;TYPE=WORK:ADR\;WORK:\;\;123 Dublin rd\,\;Oranmore\;Galway\;\;Ireland
EMAIL;TYPE=X-CUSTOM1;X LABEL=Custom:testuser01@test.com N:test;user;;; NICKNAME:pizzaguy01
ORG:ABC TEL;TYPE=WORK,VOICE:5323534535 TITLE:QA VERSION:3.0 END:VCARD
```

注意 ファイル自体のサイズや vCard 情報が破損するリスクがあるため、CSV ファイルを手動で変更しないことをお勧めします。

次の表では、非プレゼンス連絡先の入力ファイルのパラメータについて説明します。

パラメータ	説明
ユーザ JID	ユーザの JID。これは、ユーザの IM アドレスです。
コンタクト JID	連絡先リストエントリのユーザ JID(使用可能な場合)。それ以外の場合は UUID です。
グループ名	連絡先リストエントリが追加されるグループの名前。
コンテンツ タイプ	情報フィールドで使用される textmime タイプおよびサブタイプ。
バージョン	[情報(info)] フィールドで使用されるコンテンツ タイプ。
情報	VCard 形式の連絡先リストエントリの連絡先情報。

ユーザの場所の詳細をインポートするためのファイルの詳細

入力ファイルは次の形式の CSV ファイルである必要があります。

```
<User JID>、<Access Type>、<Item ID>、<Create Time>、<Resource ID>、<Message Text>
```

次に、CSV ファイル エントリのサンプルを示します。

```
userA@example.com,W,7d0ec34c-458f-4fd2-9d15-58accac4af00,2021-01-22
10:11:18.000001,jabber_7151,

<geoloc
xmlns='http://jabber.org/protocol/geoloc'><description>newlocation104</description><street>104</street><mobile>0</mobile><enable>1</enable></geoloc>
```

Caution ファイル自体のサイズやユーザの場所情報が破損するリスクがあるため、CSV ファイルを手動で変更しないことをお勧めします。

次の表に、ユーザの場所情報の入力ファイルのパラメータについて説明します。

パラメータ	説明
ユーザ JID	これは必須パラメータです。 ユーザ JID は、ユーザの IM アドレスです。これには、最大 255 文字を使用できます
アクセスタイプ	これは必須パラメータです。アクセスタイプは、ユーザのアクセスタイプを定義します。これには、最大 128 文字を使用できます。 アクセスタイプの値は次のとおりです。 • W：ホワイトリスト • R：名簿グループ • O：オープン **Note** Jabber には「W」を使用します。
アイテム ID	これは必須パラメータです。 アイテム ID は、ユーザの特定のレコードを識別します。アイテム ID の値は「無視」または英数字の値にする必要があります。連絡先リスト エントリのユーザ ID。最大 50 文字を使用できます。
Create Time	これは必須パラメータです。 [作成時間（Create Time）] には、アイテムが作成または更新された日時が表示されます。最大 26 文字を使用できます。

パラメータ	説明
リソースID	これは必須パラメータです。 リソース ID は Jabber インスタンス ID です。最大 1023 文字を使用できます。
メッセージ テキスト	これは必須パラメータです。 メッセージテキストは、ユーザの位置情報です。最大 30000 文字を使用できます。

新しい一括管理ジョブの作成

連絡先リストおよび非プレゼンス連絡先リストの新しい一括管理ジョブを作成します。

始める前に

入力ファイルのアップロード（441 ページ）

手順

Step 1 **Cisco Unified CM IM and Presence の管理：**

- 連絡先リストの新しい一括管理ジョブを作成する場合は、**一括管理** > **連絡先リスト** > **更新**を選択します
- 連絡先リストの新しいバルク管理ジョブを作成する場合は、**一括管理** > **非プレゼンス連絡先リスト** > **非プレゼンス連絡先リスト**を選択します。
- ユーザの場所を移行するための新しい一括管理ジョブを作成する場合は、**[一括管理（Bulk Administration）]** > **[ユーザの場所の移行（User Location Migration）]** > **[ユーザの場所の詳細のインポート（Import User Location Details）]** を選択します。

Step 2 [ファイル名（File Name）] ドロップダウン リストから、インポートするファイルを選択します。

Step 3 [ジョブの説明（Job Description）] フィールドに、この一括管理コミッションの説明を入力します。

Step 4 次のいずれかを実行します。

- 一括管理ジョブをただちに実行するには、[今すぐ実行（Run Immediately）] をクリックします。
- 一括管理ジョブを実行する時間をスケジュールするには、[後で実行（Run Later）] をクリックします。BAT でジョブをスケジュールする方法の詳細については、Cisco Unified CM IM and Presence の管理のオンライン ヘルプを参照してください。

Step 5 [送信（Submit）] をクリックします。ジョブをただちに実行するように選択した場合は、[送信（Submit）] をクリックするとジョブが実行されます。

次のタスク

一括管理ジョブの結果の確認 （448 ページ）

一括管理ジョブの結果の確認

一括管理ジョブが完了すると、IM and Presence サービス BAT ツールは、連絡先リストのインポート ジョブの結果をログ ファイルに書き込みます。ログ ファイルには、次の情報が含まれています。

- 正常にインポートされた連絡先の数。
- 連絡先をインポートしようとした際に発生した内部サーバ エラーの数。
- インポートされなかった（無視された）連絡先の数。ログ ファイルには、無視されたそれぞれの連絡先の理由がログ ファイルの末尾に記載されます。次に、連絡先がインポートされない理由を示します。
  - 無効な形式：無効な行形式。たとえば、必須フィールドが見つからないか、または空になっています
  - 無効なアクセス ドメイン：連絡先ドメインの形式が無効です。連絡先ドメインの有効な形式については、ユーザの連絡先リストの一括インポートに関するトピックを参照してください
  - 連絡先として自身を追加できない：連絡先がユーザの場合、そのユーザの連絡先はインポートできません
  - ユーザの連絡先リストが制限を超えている：ユーザが連絡先リストの最大サイズに達したため、これ以上の連絡先をそのユーザに対してインポートできません
  - ユーザはローカル ノードに割り当てられない：ユーザはローカル ノードに割り当てられません
- BAT ジョブを早期に終了させたエラーが原因で処理されなかった CSV ファイル内の連絡先の数。このエラーは滅多に起こりません。

このログ ファイルにアクセスするには、次の手順を実行します。

始める前に

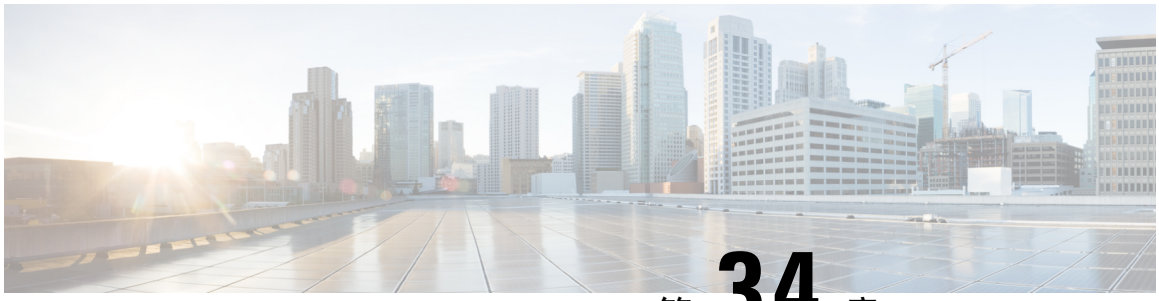
新しい一括管理ジョブの作成 （447 ページ）

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**一括管理** > **ジョブ スケジューラ**を選択します。

Step 2 **[検索（Find）]** をクリックして、連絡先リストのインポート ジョブのジョブ ID を選択します。

Step 3 **[ログ ファイル名（Log File Name）]** リンクをクリックし、ログを開きます。



第 34 章

システムのトラブルシューティング

トラブルシューティングの概要

IM and Presence の展開に関する問題のトラブル シューティングを行うには、この章の手順を使用します。IM and Presence Service の展開を使用して、以下が可能です。

- コマンドライン インターフェイス（CLI）を使用してトレース ログを作成し、問題解決に利用することができます。
- 診断を実行して、システムの問題を確認します。
- システムのトラブル シューティングを実行して、システムの状態を確認します。
- ディレクトリ URI の重複の問題のトラブル シューティングを行います。

システムのトラブル シューティングの実行

トラブル シューティングを実行して、IM and Presence Service の展開に関する問題を診断します。以下のようなさまざまな問題がトラブル シューティングで自動的に確認することができます。

- システムに関する問題
- Sync Agent の問題
- プレゼンス エンジンの問題
- SIP プロキシの問題
- 予定表の問題

- クラスタ間接続の問題
- トポロジの問題
- Cisco Jabber の冗長性の割り当て
- 外部データベース エントリ
- サードパーティ コンプライアンス サーバ
- サードパーティ LDAP 接続
- LDAP 接続
- XCP ステータス
- ユーザ設定

手順

Step 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（System Troubleshooter）]** を選択します。
このトラブル シューティングでは、システムに対して一連の自動チェックを実行します。**システム設定のトラブル シューティング** ウィンドウに結果が表示されます。

Step 2 トラブル シューティングで強調表示されている問題を解決します。

診断の実行

稼働中のシステムの管理中に、システムの通常の動作に影響を与える問題が発生する場合があります。IM and Presence Service 診断ツールを使用すると、こういったの問題の根本的な原因を特定するのに役立てられます。

IM and Presence Service の診断ツールにアクセスするには、以下の手順を使用します。

ツールにアクセスするには、**Cisco Unified CM IM and Presence 管理** で、**診断**をクリックして、以下のいずれかのオプションを選択します。

手順

Step 1 **Cisco Unified CM IM and Presence 管理**で、**診断**を選択します。

Step 2 ドロップダウン リストで、使用する診断ツールをクリックします。

これらのツールの目的の詳細については、「診断ツールの概要」を参照してください。

診断ツールの概要

診断ツール	目的
システム ダッシュボード	システムダッシュボードを使用して、これらのシステム コンポーネントの要約データ ビュー（デバイス数、ユーザー数、連絡先などのユーザー毎データ、およびプライマリ内線番号）を含む IM and Presence Service システムの状態のスナップショットを取得します。
システム設定トラブルシューティング	初期設定後または設定を変更した際に、随時 IM and Presence Service 設定の問題を診断するには、システム設定トラブルシューティングを使用します。トラブルシューティングでは、IM and Presence Service クラスタと[MISSING] 両方でテストセットを実行します。 IM and Presence Service 設定を検証するための Cisco Unified Communications Managerクラスタ。 このトラブルシュータのテストが終了すると、各テストで次の 3 つのステータスのいずれかがレポートされます。 • テスト合格 • テスト失格 • テスト警告（設定に関する問題がある可能性を示す） 不合格または警告となったテストごとに、問題点の説明と考えられる解決方法が示されます。不合格または警告となったテストごとに、解決策の列で[fix]リンクをクリックし、Cisco Unified Presence 管理ウィンドウに移動します。このウィンドウには、設定トラブルシュータで検出された問題が表示されます。見つかった設定エラーを修正して、トラブルシュータを再度実行します。

トラブルシューティングでのトレースログの使用

トレースを使用してIM and Presenceサービスおよび機能に関するシステムの問題をトラブルシューティングします。さまざまなサービス、機能、およびシステムコンポーネントに対して自動システム トレースを設定することができます。結果は、Cisco Unified Real-Time Monitoring Tool を使用して参照および表示ができるシステムログに保存されます。また、コマンドラインインターフェイスを使用して、システム ログ ファイルのサブセットを取得し、自分の PC またはラップトップにアップロードして詳細な分析を行うことも可能です。

トレースを使用するには、まずシステムをトレース用に設定する必要があります。トレースを設定する方法の詳細については、*Cisco Unified Serviceability* 管理ガイドの「トレース」の章を参照してください。

トレースの設定後、以下の 2 つの方法のいずれかを使用して、トレース ファイルの内容を表示することができます。

- Real-Time Monitoring Tool：Real-Time Monitoring Tool を使用して、システム トレースの結果として作成された個々のログ ファイルを参照および表示することができます。Real-Time Monitoring Tool の使用法の詳細については、 *Cisco Unified Real-Time Monitoring Tool* 管理ガイドを参照してください。
- コマンドラインインターフェイス（CLI）：システム トレースが設定されている場合は、CLI を使用してシステムログからカスタマイズされたトレースを作成します。CLIを使用すると、カスタマイズされたトレース ファイルに含める特定の日付の指定が可能です。CLI はシステムから関連付けられたトレース ファイルを取得して、圧縮 zip ファイルに保存して、後で分析するために、PCまたはラップトップにコピーすることができるため、システムによってログが上書きされることはありません。

  このセクションの以降の表およびタスクでは、IM and Presence Service のトレース ログ ファイルを作成するための CLI コマンドの使用方法について説明します。

トレースを使用した一般的な IM and Presence の問題

以下の表では、IM and Presence Service に関する一般的な問題および、問題をトラブルシューティングするために実行することができるトレースの一覧が説明されています。

表 *47 :* 一般的な *IM and Presence* の問題のトラブルシューティング

問題個所 ...	これらのサービスのトレースの表示	追加手順
ログイン認証	Client Profile Agent Cisco XCP Connection Manager Cisco XCP Router Cisco XCP Authentication Service Cisco Tomcat Security Logs	ログおよび出力場所を作成するための CLI コマンドは、CLIを介した共通トレース（455 ページ）を参照してください。
アベイラビリティ ステータス	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine	ログおよび出力場所を作成するための CLI コマンドは、CLIを介した共通トレース（455 ページ）を参照してください。
IM の送受信	Cisco XCP Connection Manager Cisco XCP Router	ログおよび出力場所を作成するための CLI コマンドは、CLIを介した共通トレース（455 ページ）を参照してください。
連絡先リスト	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine	ログおよび出力場所を作成するための CLI コマンドは、CLIを介した共通トレース（455 ページ）を参照してください。
チャット ルーム	Cisco XCP Connection Manager Cisco XCP Router Cisco XCP Text Conferencing Manager	ログおよび出力場所を作成するための CLI コマンドは、CLIを介した共通トレース（455 ページ）を参照してください。
パーティションイントラドメイン フェデレーション	Cisco XCP Router Cisco XCP SIP Federation Connection Manager Cisco SIP Proxy Cisco Presence Engine	ログおよび出力場所を作成するための CLI コマンドは、CLIを介した共通トレース（455 ページ）を参照してください。 （注） SIP メッセージ交換を確認するには、Cisco SIP Proxy デバッグ ログ機能が必要

問題個所 ...	これらのサービスのトレースの表示	追加手順
XMPP ベースのドメイン間フェデレーション連絡先のアベイラビリティおよび IM の問題のトレース	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine Cisco XCP XMPP Federation Connection Manager	ログおよび出力場所を作成するための CLI コマンドは、CLIを介した共通トレース（455 ページ）を参照してください。 XMPP フェデレーションが有効な各 IM and Presence Service ノードで、このトレースを実行する
SIP ドメイン間フェデレーション連絡先のアベイラビリティおよび IM の問題のトレース	Cisco XCP Connection Manager Cisco XCP Router Cisco Presence Engine Cisco SIP Proxy Cisco XCP SIP Federation Connection Manager	ログおよび出力場所を作成するための CLI コマンドは、CLIを介した共通トレース（455 ページ）を参照してください。
カレンダー トレース	Cisco Presence Engine	ログおよび出力場所を作成するための CLI コマンドは、CLIを介した共通トレース（455 ページ）を参照してください。
クラスタ間同期トレースおよびクラスタ間トラブルシューティング	Cisco Intercluster Sync Agent Cisco AXL Web Service Cisco Tomcat Security Log Cisco Syslog Agent	クラスタ間のエラーを確認するには、**診断 > システム トラブルシューティング**で、システム トラブルシューティングを実行します。
SIP フェデレーション トレース	Cisco SIP Proxy Cisco XCP Router Cisco XCP SIP Federation Connection Manager	ログおよび出力場所を作成するための CLI コマンドは、CLIを介した共通トレース（455 ページ）を参照してください。
XMPP フェデレーション トレース	Cisco XCP Router Cisco XCP XMPP Federation Connection Manager	ログおよび出力場所を作成するための CLI コマンドは、CLIを介した共通トレース（455 ページ）を参照してください。

問題個所 ...	これらのサービスのトレースの表示	追加手順
高 CPU と低 VM のアラートのトラブルシューティング	Cisco XCP Router Cisco XCP SIP Federation Connection Manager Cisco SIP Proxy Cisco Presence Engine Cisco Tomcat Security Log Cisco Syslog Agent	その他のトラブルシューティングを行うには、以下の CLI コマンドを実行します。 • `show process using-most cpu` • `show process using-most memory` • `utils dbreplication runtimestate` • `utils service list` 以下の CLI を実行して、RIS（Real-Time Information Servic）データを取得します。 • `file get activelog cm/log/ris/csv` また、Cisco Unified IM and Presence Serviceability のアラームを設定することで、実行時のステータスとシステムの状態に関する情報をローカル システムのログに提供できます。

CLIを介した共通トレース

コマンドライン インタフェースを使用して、システムのトラブルシューティングを行うためのトレース ログ ファイルを作成します。CLI を使用して、トレースを実行するコンポーネントを選択して、<duration> を指定することができます。これは、ログ ファイルに含める、その日から過去にさかのぼる日数です。

以下の 2 つの表に、トレース ログ ファイルおよびログ出力場所の作成に使用できる CLI コマンドが提示されています。

- IM and Presence サービス
- IM and Presence 機能

（注） CLI は、Cisco Unified Real-Time Monitoring Tool（RTMT）で表示可能であるのと同じ個々のトレースファイルのサブセットを取得し、グループ化して単一の圧縮 zip ファイルに格納します。RTMT トレースの詳細は、RTMT を介した共通トレース（460 ページ）を参照してください。

表 *48 : CLI* を使用した *IM and Presence Servic* の共通トレース

サービス	ログを作成するための CLI	CLI 出力ファイル
Cisco 監査ログ	file build log cisco_audit_logs <duration>	/epas/trace/log_cisco_audit_logs_*.tar.gz
Cisco Client Profile Agent	file build log cisco_client_profile_agent <duration>	/epas/trace/log_cisco_client_profile_agent_*.tar.gz
Cisco Cluster Manager	file build log cisco_config_agent <duration>	/epas/trace/log_cisco_cluster_manager_*.tar.gz
Cisco Config Agent	file build log cisco_config_agent<duration>	/epas/trace/log_cisco_config_agent_*.tar.gz
Cisco Database Layer Monitor	file build log cisco_database_layer_monitor <duration>	/epas/trace/log_cisco_database_layer_monitor_*.tar.gz
Cisco Intercluster Sync Agent	file build log cisco_inter_cluster_sync_agent <duration>	/epas/trace/log_cisco_inter_cluster_sync_agent_*.tar.gz
Cisco OAM Agent	file build log cisco_oam_agent <duration>	/epas/trace/log_cisco_oam_agent_*.gz
Cisco Presence Engine	file build log cisco_presence_engine <duration>	/epas/trace/log_cisco_presence_engine_*.tar.gz
Cisco RIS（Real-time Information Service）データコレクタ	file build log cisco_ris_data_collector <duration>	/epas/trace/log_cisco_ris_data_collector_*.tar.gz
Cisco サービス管理（CSM）	file build log cisco_service_management <duration>	/epas/trace/log_cisco_service_management_*.tar.gz
Cisco SIP Proxy	file build log cisco_sip_proxy <duration>	/epas/trace/log_cisco_sip_proxy_*.tar.gz
Cisco Sync Agent	file build log cisco_sync_agent <duration>	/epas/trace/log_cisco_sync_agent_*.tar.gz

サービス	ログを作成するための CLI	CLI 出力ファイル
Cisco XCP Config Manager	file build log cisco_xcp_config_mgr <duration>	/epas/trace/log_cisco_xcp_config_mgr_*.tar.gz
Cisco XCP Router	file build log cisco_xcp_router <duration>	/epas/trace/log_cisco_xcp_router_*.tar.gz

表 *49 : CLI* を使用した *IM and Presence* 機能の一般的なトレース

機能名	ログを作成するための CLI	CLI 出力ファイル
管理 GUI	file build log admin_ui <duration>	/epas/trace/log_admin_ui_*.tar.gz
一括管理	file build log bat <duration>	/epas/trace/log_bat_*.tar.gz
同期 HTTP 上の Bidirectional-streams	file build log bosh <duration>	/epas/trace/log_bosh_*.tar.gz
証明書	file build log certificates <duration>	/epas/trace/log_certificates_ * gz
設定 エージェント コア	file build log cfg_agent_core <duration>	/epas/trace/log_cfg_agent_core_*.tar.gz
Customer Voice Portal	file build log cvp <duration>	/epas/trace/log_cvp_*.tar.gz
ディレクトリ グループ	file build log directory_groups <duration>	/epas/trace/log_directory_groups_*.tar.gz
ディザスタ リカバリ	file build log disaster_recovery <duration>	/epas/trace/log_disaster_recovery_*.tar.gz
柔軟なIM アドレス	file build log flexable_im_address <duration>	/epas/trace/log_flexible_im_address_*.tar.gz
汎用コア	file build log general_core <duration>	/epas/trace/log_general_core_*.tar.gz
ハイ アベイラビリティ	file build log ha <duration>	/epas/trace/log_ha_*.tar.gz
高いCPU使用率	file build log high_cpu <duration>	/epas/trace/log_high_cpu_*.tar.gz
ハイ メモリ	file build log high_memory <duration>	/epas/trace/log_high_memory_*.tar.gz
インスタント メッセージング データベース コア	file build log imdb <duration>	/epas/trace/log_imdb_core_*.tar.gz

機能名	ログを作成するための CLI	CLI 出力ファイル
クラスタ間ピアリング	file build log inter_cluster <duration>	/epas/trace/log_inter_cluster_*.tar.gz
マネージド ファイル転送	file build log managed_file_transfer <duration>	/epas/trace/log_managed_file_transfer_*.tar.gz
Microsoft Exchange	file build log msft_exchange <duration>	/epas/trace/log_msft_exchange_ * gz
メッセージ アーカイバ	file build log msg_archiver <duration>	/epas/trace/log_msg_archiver_*.tar.gz
プレゼンス エンジン コア	file build log pe_core <duration>	/epas/trace/log_pe_core_*.tar.gz
Presence and IM メッセージ交換	file build log presence_im_exchange <duration>	/epas/trace/log_presence_im_exchange_*.tar.gz
SIP ログインの問題	file build log pws <duration>	/epas/trace/log_pws_*.tar.gz
セキュリティの脆弱性	file build log sec_vulnerability <duration>	/epas/trace/log_sec_vulnerability_*.tar.gz
サービスアビリティの GUI	file build log serviceability_ui <duration>	/epas/trace/log_serviceability_ui_*.tar.gz
SIP ドメイン間フェデレーション	file build log sip_inter_federation <duration>	/epas/trace/log_sip_inter_federation_ * tar.gz
SIP パーティション ドメイン間 フェデレーション	file build log sip_partitioned_federation <duration>	/epas/trace/log_sip_partitioned_federation_ *.tar.gz
SIP プロキシ コア	file build log sipd_core <duration>	/epas/trace/log_sipd_core_*.tar.gz
常設チャットのハイ アベイラビリティ	file build log tc_ha <duration>	/epas/trace/log_tc_ha_*.tar.gz
永続的なチャット	file build log text_conference <duration>	/epas/trace/log_text_conference_*.tar.gz
アップグレードの問題	file build log upgrade_issues <duration>	/epas/trace/log_upgrade_issues_*.tar.gz
□ユーザ接続	file build log user_connectivity <duration>	/epas/trace/log_user_connectivity_*.tar.gz
名簿	file build log user_rosters <duration>	/epas/trace/log_user_rosters_*.tar.gz

機能名	ログを作成するための CLI	CLI 出力ファイル
XCP ルータ コア	file build log xcp_core <duration>	/epas/trace/log_xcp_core_*.tar.gz
XMPP ドメイン間フェデレーション	file build log xmpp_inter_federation <duration>	/epas/trace/log_xmpp_inter_federation_*.tar.gz
展開情報	file build log deployment_info <duration>	/epas/trace/log_deployment_info_*.tar.gz

CLI 経由のトレースの実行

CLI（コマンドライン インターフェイス）を介してカスタマイズしたトレース ファイルを作成するには、次の手順を使用します。CLI で duration パラメータを使用して、トレースに含める過去にさかのぼる日数を指定することができます。CLI は、システム ログのサブセットを取得します。

（注） SFTP サーバーは、ファイル転送にのみに使用してください。

始める前に

システムにトレースが設定されている必要があります。トレースを設定する方法の詳細は、*Cisco Unified Serviceability* 管理ガイド の「Traces」の章を参照してください。

実行可能なトレースのリストを CLIを介した共通トレース （455 ページ） で確認します。

手順

Step 1 コマンドライン インターフェイスにログインします。

Step 2 ログを作成するには、`file build log <name of service> <duration>` CLI コマンドを実行します。duration には、トレースに含める日数を指定します。

たとえば、`file build log cisco_cluster_manager 7` では、Cisco Cluster Manager ログの過去 1 週間分を表示します。

Step 3 ログを取得するには、`file get activelog <log filepath>` CLI コマンドを実行します。

たとえば、**file get activelog epas/trace/log_cisco_cluster_manager__2016-09-30-09h41m37s.tar.gz**となります。

Step 4 システムの安定性を維持するために、取得後にログは削除します。ログを削除するには、`file delete activelog <filepath>` コマンドを実行します。

たとえば、`file delete activelog epas/trace/log_cisco_cluster_manager__2016-09-30-09h41m37s.tar.gz`となります。

RTMT を介した共通トレース

次の表に、IM and Presence Service ノードと結果のログ ファイルで実行できる共通トレースを示します。Real-Time Monitoring Tool（RTMT）を使用してトレース ログ ファイルを表示することができます。

（注） CLI を使用すると、RTMT で表示可能であるのと同じ個々のトレース ファイルのサブセットを取得することができ、単一の圧縮 zip ファイルにまとめて保存することが可能です。CLI トレースの詳細は、CLIを介した共通トレース （455 ページ）を参照してください。

表 *50 : IM and Presence Service* ノードに共通のトレースおよびトレース ログ ファイル

サービス	トレース ログのファイル名
Cisco AXL Web サービス	`/tomcat/logs/axl/log4j/axl*.log`
Cisco Intercluster Sync Agent	`/epas/trace/cupicsa/log4j/icSyncAgent*.log`
Cisco Presence Engine	`/epas/trace/epe/sdi/epe*.txt.gz`
Cisco SIP Proxy	`/epas/trace/esp/sdi/esp*.txt.gz`
Cisco Syslog Agent	`/cm/trace/syslogmib/sdi/syslogmib*.txt`
Cisco Tomcat Security Log	`/tomcat/logs/security/log4/security*.log`
Cisco XCP Authentication Service	`/epas/trace/xcp/log/auth-svc-1*.log.gz`
Cisco XCP Config Manager	`/epas/trace/xcpconfigmgr/log4j/xcpconfigmgr*.log`
Cisco XCP Connection Manager	`/epas/trace/xcp/log/client-cm-1*.log.gz`
Cisco XCP Router	`/epas/trace/xcp/log/rtr-jsm-1*.log.gz`
Cisco XCP SIP Federation Connection Manager	`/epas/trace/xcp/log/sip-cm-3*.log`
Cisco XCP Text Conferencing Manager	`/epas/trace/xcp/log/txt-conf-1*.log.gz`
Cisco XCP XMPP Federation Connection Manager	`/epas/trace/xcp/log/xmpp-cm-4*.log`
Cluster Manager	`/platform/log/clustermgr*.log`

サービス	トレース ログのファイル名
Cisco Client Profile Agent（CPA）	/tomcat/logs/epassoap/log4j/EPASSoap*.log
dbmon	/cm/trace/dbl/sdi/dbmon*.txt

ユーザ ID エラーおよびディレクトリ URI エラーのトラブルシューティング

重複したユーザ ID エラーの受信

問題 ユーザ ID が重複していることを示すアラームを受信しました。これらのユーザの連絡先情報を修正しなければなりません。

解決法 次のステップを実行します。

1. **utils users validate { all | userid | uri }** CLI command を使用して、すべてのユーザのリストを生成します。CLI の使用の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

   ユーザ ID に続いて重複したユーザ ID の元となっているサーバのリストが、結果セットに表示されます。次の CLI 出力の例は、出力時のユーザ ID エラーを示しています。

   ```
   Users with Duplicate User IDs
   ---------------------------------------------
    User ID: user3
     Node Name
     cucm-imp-1
     cucm-imp-2
   ```

2. 同じユーザが 2 台の別のクラスタに割り当てられている場合、いずれかのクラスタからそのユーザの割り当てを解除します。
3. 別のクラスタで異なるユーザに同じユーザ ID が割り当てられている場合、いずれかのユーザに対しユーザ ID 値の名前を変更して、重複がないようにします。
4. ユーザ情報が無効または空白の場合、Cisco Unified Communications Manager Administration の GUI を使用して、そのユーザのユーザ ID 情報を修正します。
5. Cisco Unified Communications Manager 内のユーザ レコードを修正できます。[エンド ユーザの設定（End User Configuration）] ウィンドウ（**[ユーザの管理（User Management）]** > **[エンド ユーザ（EndUser）]**）を使用することで、必要に応じて、全ユーザに有効なユーザ ID またはディレクトリ URI 値を確実に設定します。詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

（注） ユーザ プロファイルの [ユーザ ID（User ID）] フィールドと [ディレクトリ URI（Directory URI）] フィールドが LDAP ディレクトリにマップされている場合があります。その場合は、 LDAP ディレクトリ サーバで修正を適用します。

6. 重複したユーザ ID エラーがそれ以上ないことを確認するには、CLI コマンドをもう一度実行してユーザを検証します。

重複または無効なディレクトリ URI エラーの受信

問題 ユーザ ディレクトリ URI が重複または無効であることを示すアラームを受信しました。これらのユーザの連絡先情報を修正しなければなりません。

解決法 次のステップを実行します。

1. **utils users validate { all | userid | uri }** CLI command を使用して、すべてのユーザのリストを生成します。CLI の使用の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

   ディレクトリ URI の値、続いて重複または無効なディレクトリ URI の元となっているサーバのリストが、結果セットに表示されます。次の CLI 出力の例は、検証チェック時に検出されたディレクトリ URI エラーを示しています。

```
Users with No Directory URI Configured
-------------------------------------------------------
 Node Name: cucm-imp-2
 User ID
 user4

Users with Invalid Directory URI Configured
-------------------------------------------------------
 Node Name: cucm-imp-2
 User ID   Directory URI
 user1     asdf@ASDF@asdf@ADSF@cisco

Users with Duplicate Directory URIs
-------------------------------------------------------
Directory URI: user1@cisco.com
 Node Name   User ID
 cucm-imp-1  user4
 cucm-imp-2  user3
```

2. 同じユーザが 2 台の別のクラスタに割り当てられている場合、いずれかのクラスタからそのユーザの割り当てを解除します。

3. 別のクラスタで異なるユーザに同じディレクトリ URI が割り当てられている場合、いずれかのユーザに対しディレクトリ URI 値の名前を変更して、重複がないようにします。

4. ユーザ情報が無効または空白の場合、ユーザのディレクトリ URI 情報を修正します。

5. Cisco Unified Communications Manager 内のユーザ レコードを修正できます。[エンド ユーザの設定（End User Configuration）] ウィンドウ（**[ユーザの管理（User Management）] > [エンド ユーザ（EndUser）]**）を使用することで、必要に応じて、全ユーザに有効なユーザ ID または

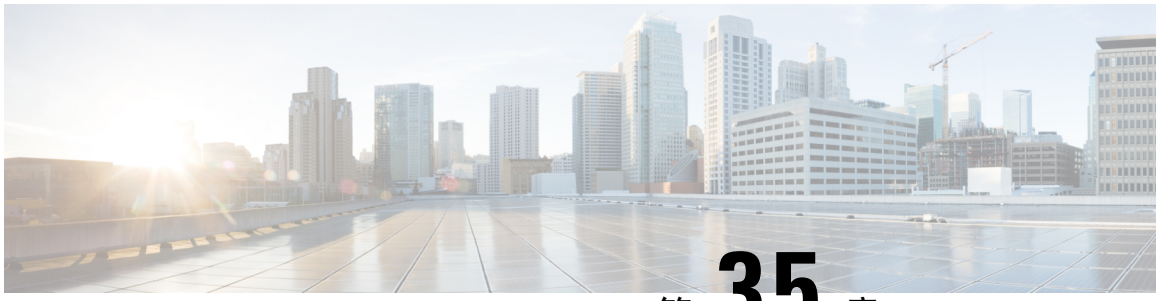
ディレクトリ URI 値を確実に設定します。詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

（注） ユーザ プロファイルの [ユーザ ID（User ID）] フィールドと [ディレクトリ URI（Directory URI）] フィールドが LDAP ディレクトリにマップされている場合があります。その場合は、 LDAP ディレクトリ サーバで修正を適用します。

6. 重複または無効なディレクトリ URI エラーがそれ以上ないことを確認するには、CLI コマンドをもう一度実行してユーザを検証します。

第 V 部

参考情報



第 35 章

Cisco Unified Communications Manager の TCP および UDP ポートの使用

この章では、Cisco Unified Communications Manager がクラスタ内接続および外部アプリケーションまたはデバイスとの通信に使用する TCP ポートと UDP ポートの一覧を示します。また、IP Communications ソリューションの実装時に、ネットワークにファイアウォール、アクセス コントロール リスト（ACL）、および Quality of Service（QoS）を設定するために重要な情報も記載されています。

Cisco Unified Communications Manager の TCP と UDP ポートの使用に関する概要

Cisco Unified Communications Manager の TCP および UDP ポートは、次のカテゴリに整理されます。

- Cisco Unified Communications Manager サーバーがクラスタ間で使用するポート
- 共通サービス ポート
- Cisco Unified Communications Manager と LDAP ディレクトリの間のポート
- CCMAdmin または CCMUser から Cisco Unified Communications Manager への Web 要求
- Cisco Unified Communications Manager から電話機への Web 要求
- 電話機と Cisco Unified Communications Manager の間のシグナリング、メディア、およびその他の通信
- ゲートウェイと Cisco Unified Communications Manager の間のシグナリング、メディア、およびその他の通信

- アプリケーションと Cisco Unified Communications Manager の間の通信
- CTL クライアントとファイアウォールの通信
- HP サーバ上の特殊なポート

上記のそれぞれのカテゴリのポートの詳細については、「「ポートの説明」」を参照してください。

（注） シスコでは、これらのポートで想定されるすべての設定シナリオを検証しているわけではありません。この一覧を参考にした結果、設定に問題が発生した場合は、シスコのテクニカルサポートにお問い合わせください。

ポート設定は、特に Cisco Unified Communications Manager に適用されます。リリースによってポートが異なる場合があり、今後のリリースで新しくポートが追加される可能性もあります。このため、インストールされている Cisco Unified Communications Manager のバージョンに一致するバージョンのマニュアルを使用していることを確認してください。

事実上すべてのプロトコルが双方向で行われますが、セッション開始側から見た方向を記載しています。デフォルトのポート番号は、管理者が手動で変更できる場合もありますが、ベスト プラクティスとしてこのような変更は推奨しません。Cisco Unified Communications Manager が内部使用に限って複数のポートを開くことに注意してください。

Cisco Unified Communications Manager ソフトウェアをインストールすると、デフォルトでは有用性のために次のネットワーク サービスが自動的にインストールされてアクティブになります。詳細については、「Cisco Unified Communications Manager サーバの間のクラスタ内ポート」を参照してください。

- Cisco Log Partition Monitoring（共通パーティションを監視および消去します。このサービスは、カスタム共通ポートを使用しません）
- Cisco Trace Collection Service（TCTS ポート使用）
- Cisco RIS Data Collector（RIS サーバ ポート使用）
- Cisco AMC Service（AMC ポート使用）

ファイアウォール、ACL、または QoS の設定は、トポロジ、テレフォニー デバイスおよびテレフォニー サービスの配置とネットワーク セキュリティ デバイスの配置との関係、および使用中のアプリケーションとテレフォニー拡張機能によって異なります。また、デバイスやバージョンによって、ACL のフォーマットが異なることにも注意してください。

（注） Cisco Unified Communications Manager でマルチキャスト保留音（MoH）ポートを設定することもできます。このマニュアルにはマルチキャスト MOH のポート値を記載していません。

（注） システムのエフェメラル ポートの範囲は 32768 ～ 61000 であり、電話を登録したままにするには、これらのポートを開く必要があります。詳細については、「http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html」を参照してください。

（注） ポート 22 への接続が開き、抑えられないように、ファイアウォールを設定します。IM and Presence サブスクライバ ノードのインストール中に、Cisco Unified Communications Manager パブリッシャ ノードに対する複数の接続が短時間に連続して開かれます。これらの接続をスロットリングすると、インストールが失敗する可能性があります。

ポート説明

Cisco Unified Communications Manager サーバーがクラスタ間で使用するポート

表 *51 : Cisco Unified Communications Manager* サーバーがクラスタ間で使用するポート

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
エンドポイント	Unified Communications Manager	514 / UDP	システム ロギング
エンドポイント	Unified Communications Manager	514 / UDP	システム ロギング
Unified Communications Manager	Unified Communications Manager	443 / TCP	このポートは、サブバノードでの COP のインストール中にクライバとパブリッ通信に使用されます
Unified Communications Manager	RTMT	1090、1099 / TCP	RTMT パフォーマンター、データ収集、グ、およびアラート Cisco AMC サービス
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1500、1501 / TCP	データベース接続 TCP はセカンダリ接
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1510 / TCP	CAR IDS DB。CAR ジンが、クライアン接続要求を監視しま
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1511 / TCP	CAR IDS DB。アッド時に、CAR IDS のタンスをもう 1 つ開めに使用される代替
Unified Communications Manager（DB）	Unified Communications Manager（DB）	1515 / TCP	インストール時のノのデータベース レプション
Cisco Extended Functions（QRT）	Unified Communications Manager（DB）	2552 / TCP	Cisco Unified Commu Managerデータベー知をサブスクライバきるようにします。
Unified Communications Manager	Unified Communications Manager	2551 / TCP	アクティブ/バック別のための Cisco Ex Services 間のクラス

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager（RIS）	Unified Communications Manager（RIS）	2555 / TCP	Real-time Informa（RIS）データベ バー
Unified Communications Manager（RTMT、AMC、またはSOAP）	Unified Communications Manager（RIS）	2556 / TCP	Cisco RIS 向け R Information Servi データベース ク
Unified Communications Manager（DRS）	Unified Communications Manager（DRS）	4040 / TCP	DRS プライマリ ト
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5001 / TCP	このポートは、 ターがリアルタ ターリング サー します。
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5002 / TCP	このポートは、 ターがパフォー ター サービスに す。
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5003 / TCP	このポートは、 ターがコントロ ター サービスに す。
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5004 / TCP	このポートは、 ターがログ コレ サービスに使用
標準 CCM 管理者ユーザ / 管理者	Unified Communications Manager	5005 / TCP	このポートは SO CDROnDemand2 よって使用され
Unified Communications Manager（Tomcat）	Unified Communications Manager（SOAP）	5007 / TCP	SOAP モニター
Unified Communications Manager（RTMT）	Unified Communications Manager（TCTS）	エフェメラル / TCP	Cisco Trace Colle Service（TCTS） Trace and Log Cen 向けのバックエ ス
Unified Communications Manager（Tomcat）	Unified Communications Manager（TCTS）	7000、7001、7002 / TCP	このポートは、 Collection Tool S Cisco Trace Colle との通信に使用

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager	証明書マネージャ	7070 / TCP	証明書マネージャ
Unified Communications Manager（DB）	Unified Communications Manager（CDLM）	8001 / TCP	クライアント デー 変更通知
Unified Communications Manager（SDL）	Unified Communications Manager（SDL）	8002 / TCP	クラスタ間通信サー
Unified Communications Manager（SDL）	Unified Communications Manager（SDL）	8003 / TCP	クラスタ間通信サー （CTI 対象）
Unified Communications Manager	CMI マネージャ	8004 / TCP	Cisco Unified Commu Manager と CMI マネ とのクラスタ間通信
Unified Communications Manager（Tomcat）	Unified Communications Manager（Tomcat）	8005 / TCP	Tomcat シャットダウ リプトで使用される ニング ポート
Unified Communications Manager（Tomcat）	Unified Communications Manager（Tomcat）	8080 / TCP	診断テストのための 間の通信
ゲートウェイ	Unified Communications Manager	8090	CUCM と GW（Cay ターフェイス）が C Recording 機能のた に使用する HTTP ポ
Unified Communications Manager	ゲートウェイ		
Unified Communications Manager（IPSec）	Unified Communications Manager（IPSec）	8500 / TCP および UDP	IPSec クラスタ マネ よるシステム デー スタ間複製
Unified Communications Manager（RIS）	Unified Communications Manager（RIS）	8888 ～ 8889 / TCP	RIS サービス マネー ステータス要求と応
Location Bandwidth Manager（LBM）	Location Bandwidth Manager（LBM）	9004 / TCP	LBM 間のクラスタ
Unified Communications Manager（Dialed Number Analyzer（DNA）初期化サーバー）	JNIWrapper サーバー	30000 / TCP	Dialed Number Analy （DNA） DNA の初期化を処 サーバーで使用され ト。JNIWrapper の DNA Java サービス る要求に応答しま

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager パブリッシャ	Unified Communications Manager サブスクライバ	22 / TCP	Cisco SFTP サー スクライバを新 トールする場合 トを開く必要が
Unified Communications Manager	Unified Communications Manager	8443 / TCP	ノード間のコン ター機能とネッ ビスへのアクセ ます。

共通サービス ポート

表 *52 :* 共通サービス ポート

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
エンドポイント	Unified Communications Manager	7	Internet Control Message Protocol（ICMP）。このプロトコル番号がエコー関連のトラフィックを伝送します。列見出しに示すようなポートとなるものではありません。
Unified Communications Manager	エンドポイント		
Unified Communications Manager (DRS、コール詳細レコード)	SFTP サーバー	22 / TCP	SFTP サーバーにバックアップ データを送信します。（DRS ローカル エージェント） コール詳細レコードデータを SFTP サーバーに送信します。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
エンドポイント	Unified Communications Manager（DNS サーバー）	エフェメラル / UDP	DNS サーバーまたは DNS クライアントとして機能する Cisco Unified Communications Manager （注） Cisco Unified Communications Manager を DNS サーバーとして機能させないこと、およびすべての IP テレフォニー アプリケーションおよびエンドポイントでホスト名ではなく固定 IP アドレスを使用することを推奨します。
Unified Communications Manager	DNS サーバー		
エンドポイント	Unified Communications Manager（DHCP サーバー）	67 / UDP	DHCP サーバーとして機能する Cisco Unified Communications Manager （注） Cisco Unified Communications Manager 上で DHCP サーバーを実行することは推奨しません。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager	DHCP サーバー	68 / UDP	DHCP クライアントとして機能する Cisco Unified Communications Manager （注） Cisco Unified Communications Manager 上で DHCP クライアントを実行することは推奨しません。その代わりに、Cisco Unified Communications Manager には固定 IP アドレスを設定します。
エンドポイントまたはゲートウェイ	Unified Communications Manager	69、6969、次にエフェメラル / UDP	電話、ゲートウェイへの TFTP サービス
エンドポイントまたはゲートウェイ	Unified Communications Manager	6970 / TCP	プライマリサーバーとプロキシサーバー間の TFTP。 電話機とゲートウェイに対する TFTP サーバーの HTTP サービス
Unified Communications Manager	NTP サーバー	123 / UDP	Network Time Protocol（NTP）
SNMP サーバー	Unified Communications Manager	161 / UDP	SNMP サービス応答（管理アプリケーションからの要求）
CUCM サーバ SNMP プライマリ エージェント アプリケーション	SNMP トラップの宛先	162 / UDP	SNMP トラップ
SNMP サーバー	Unified Communications Manager	199 / TCP	SMUX サポート用組み込み SNMP エージェントリスニングポート
Unified Communications Manager	DHCP サーバー	546 / UDP	DHCPv6。IPv6 用の DHCP ポート。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager Serviceability	Location Bandwidth Manager（LBM）	5546 / TCP	Enhanced Location CAC Serviceability
Unified Communications Manager	Location Bandwidth Manager（LBM）	5547 / TCP	コール アドミッションの要求および帯域幅の縮小
Unified Communications Manager	Unified Communications Manager	6161 / UDP	プライマリエージェントとネイティブエージェント間の通信に使用され、ネイティブエージェントの MIB 要求を処理します。
Unified Communications Manager	Unified Communications Manager	6162 / UDP	プライマリエージェントとネイティブエージェント間の通信に使用され、ネイティブエージェントから生成された通知を転送します。
Unified Communications Manager	Unified Communications Manager	6666 / UDP	Netdump サーバー
中央集中型 TFTP	代替 TFTP（Alternate TFTP）	6970 / TCP	中央集中型 TFTP ファイル ロケータ サービス
Unified Communications Manager	Unified Communications Manager	7161 / TCP	SNMP プライマリエージェントとサブエージェント間の通信に使用されます。
SNMP サーバー	Unified Communications Manager	7999 / TCP	Cisco Discovery Protocol（CDP）エージェントが、CDP 実行可能機器と通信します。
エンドポイント	Unified Communications Manager	443、8443/TCP	Cisco ユーザー データ サービス（UDS）の要求に使用されます。
Unified Communications Manager	Unified Communications Manager	9050 / TCP	Cisco Unified Communications Manager にある TAPS を利用して CRS 要求を処理します。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager	Unified Communications Manager	61441 / UDP	Cisco Unified Communications Manager アプリケーションが、UDP でこのポートにアラームを送信します。Cisco Unified Communications Manager MIB エージェントが、Cisco Unified Communications Manager MIB 定義に従って、このポートを監視し、SNMP トラップを生成します。
Unified Communications Manager	Unified Communications Manager	5060、5061 / TCP	トランクベースの SIP サービスを提供します。
Unified Communications Manager	Unified Communications Manager	7501	クラスタ間検索サービス（ILS）の証明書ベースの認証に使用されます。
Unified Communications Manager	Unified Communications Manager	7502	ILS がパスワードベースの認証に使用します。
Unified Communications Manager	Unified Communications Manager	9,966	ファイアウォールが有効になっているときに、クラスタ内のノード間で通信するために Cisco プッシュ通知サービスによって使用されます。
Unified Communications Manager	Unified Communications Manager	9560	ローカルプッシュ通知サービス（LPNS）で使用されます。
--	--	8000-48200	ASR および ISR G3 プラットフォームでは、デフォルトのポート範囲が指定されています。
		16384 ～ 32766	ISR G2 プラットフォームのデフォルトポート範囲。

Cisco Unified Communications Manager と LDAP ディレクトリの間のポート

表 *53 : Cisco Unified Communications Manager* と *LDAP* ディレクトリの間のポート

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager	外部ディレクトリ	389、636、3268、3269/TCP	外部ディレクトリ（Active Directory、Netscape Directory）への Lightweight Directory Access Protocol（LDAP）クエリー
外部ディレクトリ	Unified Communications Manager	エフェメラル	

CCMAdmin または CCMUser から Cisco Unified Communications Manager への Web 要求

表 *54 : CCMAdmin* または *CCMUser* から *Cisco Unified Communications Manager* への *Web* 要求

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
ブラウザ	Unified Communications Manager	80、8080/TCP	ハイパーテキスト転コル（HTTP）
ブラウザ	Unified Communications Manager	443、8443/TCP	Hypertext Transport over SSL（HTTPS）
ブラウザ	Unified Communications Manager	9463 / TCP	Hypertext Transport over SSL（HTTPS） TLS1.3 の v6 のみが です。
ブラウザまたは CLI	Unified Communications Manager	2355、2356/TCP	CLI および Web アプ ションからの監査イ ログに記録
Unified Communications Manager	Cisco License Manager	5555/TCP	Cisco License Manag のポートでのライセ をリッスンします

Cisco Unified Communications Manager から電話機への Web 要求

表 *55 : Cisco Unified Communications Manager* から電話機への *Web* 要求

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager • QRT • RTMT • [電話の検索と一覧表示（Find and List Phones）] ページ • [電話の設定（Phone Configuration）] ページ	電話	80/TCP	ハイパーテキスコル（HTTP）

電話機と Cisco Unified Communications Manager の間のシグナリング、メディア、およびその他の通信

表 *56 :* 電話機と *Cisco Unified Communications Manager* の間のシグナリング、メディア、およびその他の通信

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
電話	DNS サーバー	53 / TCP	Session Initiation Protocol（SIP）電話機が、ドメインネーム システム（DNS）を使用して、完全修飾ドメイン名（FQDN）を解決します。 （注） デフォルトでは、一部のワイヤレス アクセス ポイントは TCP の 53 番ポートをブロックし、FQDN を使用しながら CUCM を設定しているときに、ワイヤレス SIP 電話機が登録されないようにします。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
電話	Unified Communications Manager（TFTP）	69、次にエフェメラル / UDP	ファームウェアおよび設定ファイルのダウンロードに使用される Trivial File Transfer Protocol（TFTP）
電話	Unified Communications Manager	2000 / TCP	Skinny Client Control Protocol（SCCP）
電話	Unified Communications Manager	2443 / TCP	Secure Skinny Client Control Protocol（SCCPS）
電話	Unified Communications Manager	2445 / TCP	エンドポイントに信頼検証サービスを提供します。
電話	Unified Communications Manager（CAPF）	3804 / TCP	ローカルで有効な証明書（LSC）を IP 電話に発行するための認証局プロキシ機能（CAPF）リスニング ポート
電話	Unified Communications Manager	5060 / TCP および UDP	Session Initiation Protocol（SIP）電話機
Unified Communications Manager	電話		
電話	Unified Communications Manager	5061 TCP	Secure Session Initiation Protocol（SIPS）電話機
Unified Communications Manager	電話		
電話	Unified Communications Manager（TFTP）	6970 TCP	ファームウェアおよび設定ファイルの HTTP ベースのダウンロード
電話	Unified Communications Manager（TFTP）	6971、6972 / TCP	TFTP への HTTPS インターフェイス。電話機が、TFTP からセキュアな設定ファイルをダウンロードするためにこのポートを使用します。
電話	Unified Communications Manager	8080 / TCP	XML アプリケーション、認証、ディレクトリ、サービスなどの電話 URL。これらのポートをサービス単位で設定できます。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
電話	Unified Communications Manager	9443 / TCP	電話機が、認証された連絡先検索にこのポートを使用します。
電話	Unified Communications Manager	9444	電話は、このポート番号を使用してヘッドセット管理機能を利用します。
iPhone/iPad（Webex アプリ）	Unified Communications Manager	9560/セキュア WebSocket	Webex アプリは、LPNS 機能にこのポート番号を使用します。
IP VMS	電話	16384 ～ 32767 / UDP	Real-Time Protocol（RTP）、Secure Real-Time Protocol（SRTP） （注） 他のデバイスは全範囲を使用しますが、Cisco Unified Communications Manager は 24576 ～ 32767 だけを使用します。
電話	IP VMS		

ゲートウェイと Cisco Unified Communications Manager の間のシグナリング、メディア、およびその他の通信

表 *57 :* ゲートウェイと *Cisco Unified Communications Manager* の間のシグナリング、メディア、およびその他の通信

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
ゲートウェイ	Unified Communications Manager	47、50、51	Generic Routing E （GRE）、Encap Security Payload 証ヘッダー（AH のプロトコル番号 された IPSec トラ 伝送します。列見 ようなポートとか ありません。
Unified Communications Manager	ゲートウェイ		

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
ゲートウェイ	Unified Communications Manager	500 / UDP	IP Security（IPSec）ル確立のためのイン ト キー エクスチェ（IKE）
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager（TFTP）	69、次にエフェメラル/UDP	トリビアル ファイル ロトコル（TFTP）
Cisco Intercompany Media Engine（CIME）トランクを使用した Unified Communications Manager	CIME ASA	1024 ～ 65535 / TCP	ポート マッピング ス。CIME オフパス ルでのみ使用しま
Gatekeeper	Unified Communications Manager	1719 / UDP	ゲートキーパー（H RAS
ゲートウェイ	Unified Communications Manager	1720 / TCP	H.323 ゲートウェイ ラスタ間トランク けの H.225 シグナリ サービス
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	エフェメラル / TCP	ゲートキーパー制御 上の H.225 シグナリ サービス
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	エフェメラル / TCP	音声、ビデオ、およ を確立するための H ナリング サービス （注） ゲートウ 種類によ なる、リ システム される H ポート。 IOS ゲー イでの H ポート範 11000 ～ です。
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	2000 / TCP	Skinny Client Contro（SCCP）

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
ゲートウェイ	Unified Communications Manager	2001 / TCP	Cisco Unified Co Manager の導入 6608 ゲートウェ グレード ポート
ゲートウェイ	Unified Communications Manager	2002 / TCP	Cisco Unified Co Manager の導入 6624 ゲートウェ グレード ポート
ゲートウェイ	Unified Communications Manager	2427 / UDP	Media Gateway C Protocol（MGCP ウェイ コントロ
ゲートウェイ	Unified Communications Manager	2428 / TCP	Media Gateway C Protocol（MGCP ホール
--	--	4000 ～ 4005 / TCP	Cisco Unified Co Manager に音声、 よび D チャネル ないときには、 トがこのような ファントム Real Transport Protoco ポートおよび Re Transport Control （RTCP）ポート されます。
ゲートウェイ	Unified Communications Manager	5060 / TCP および UDP	Session Initiation （SIP）ゲートウ クラスタ間トラ
Unified Communications Manager	ゲートウェイ		
ゲートウェイ	Unified Communications Manager	5061 / TCP	Secure Session In Protocol（SIPS） イおよびクラス （ICT）
Unified Communications Manager	ゲートウェイ		

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
ゲートウェイ	Unified Communications Manager	16384 ～ 32767 / UDP	Real-Time Protocol（ Secure Real-Time Pro （SRTP） （注） 他のデバ 全範囲を ますが、 Unified Commun Manager ～ 32767 使用しま
Unified Communications Manager	ゲートウェイ		

アプリケーションと Cisco Unified Communications Manager の間の通信

表 *58* : アプリケーションと *Cisco Unified Communications Manager* の間の通信

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
CTL クライアント	Unified Communications Manager CTL プロバイダ	2444 / TCP	Cisco Unified Commu Managerの証明書信 （CTL）プロバイダ ング サービス
Cisco Unified Communications アプリケーション	Unified Communications Manager	2748 / TCP	CTI アプリケーショ バー
Cisco Unified Communications アプリケーション	Unified Communications Manager	2749 / TCP	CTI アプリケーショ （JTAPI/TSP）と C Manager 間の TLS 接
Cisco Unified Communications アプリケーション	Unified Communications Manager	2789 / TCP	JTAPIアプリケーシ バー
Unified Communications Manager Assistant Console	Unified Communications Manager	2912 / TCP	Cisco Unified Commu Manager Assistant サ （以前の IPMA）
Unified Communications Manager Attendant Console	Unified Communications Manager	1103 ～ 1129 / TCP	Cisco Unified Commu Manager Attendant C （AC）JAVA RMI リ サーバー

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager Attendant Console	Unified Communications Manager	1101 / TCP	RMI サーバーは ルバック メッセ らのポートを使用 アントに送信し
Unified Communications Manager Attendant Console	Unified Communications Manager	1102 / TCP	Attendant Console サーバー バイン RMI サーバーは ポートに RMI メ 送信します。
Unified Communications Manager Attendant Console	Unified Communications Manager	3223 / UDP	Cisco Unified Co Manager Attendan （AC）サーバー ポートは、Atten サーバーから pi 録メッセージを Attendant Consol 回線状態を送信
Unified Communications Manager Attendant Console	Unified Communications Manager	3224 / UDP	Cisco Unified Co Manager Attendan （AC）クライア 線状態情報およ 態情報のために に登録されます
Unified Communications Manager Attendant Console	Unified Communications Manager	4321 / UDP	Cisco Unified Co Manager Attendan （AC）クライア コール制御のた バーに登録され
SAF/CCD を使用する Unified Communications Manager	SAF イメージを実行する IOS ルータ	5050 / TCP	EIGRP/SAF プロ 行するマルチサ ルータ。
Unified Communications Manager	Cisco Intercompany Media Engine（IME）サーバー	5620 / TCP このポートでは、ポート番号 5620 の使用を推奨しますが、CLI コマンドの add ime vapserver または set ime vapserver port を Cisco IME サーバーで実行することにより、値を変更できます。	VAP プロトコル Intercompany Me サーバーとの通信 ます。

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Cisco Unified Communications アプリケーション	Unified Communications Manager	8443 / TCP	課金アプリケーショ テレフォニー管理ア ションなどのサード が、Cisco Unified Communications Mar タベースに対してプ で読み書きするため る AXL/SOAP API。

CTL クライアントとファイアウォールの通信

表 *59 : CTL* クライアントとファイアウォールの通信

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
CTL クライアント	TLS プロキシ サーバ	2444 / TCP	ASA ファイアウォ 明書信頼リスト（C バイダー リスニン ス

Cisco Smart Licensing Service と Cisco Smart Software Manager 間の通信

Unified Communications Manager の Cisco Smart Licensing Service は、Call Home を介して Cisco Smart Software Manager との直接通信を設定します。

***Table 60: Cisco Smart Licensing Service* と *Cisco Smart Software Manager* 間の通信**

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
Unified Communications Manager（Cisco Smart Licensing Service）	Cisco Smart Software Manager（CSSM）	443 / HTTPS	Smart Licensing Service はライセンスの使用状況を CSSM に送信して、Unified CM が問題であるかどうかを確認します。

HP サーバ上の特殊なポート

表 *61 : HP* サーバ上の特殊なポート

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
エンドポイント	HP SIM	2301/TCP	HP エージェント ポート
エンドポイント	HP SIM	2381/TCP	HP エージェント ポート
エンドポイント	Compaq 管理エージェント	25375、25376、25393/UDP	COMPAQ 管理エ 拡張（cmaX）
エンドポイント	HP SIM	50000 ～ 50004/TCP	HP SIM への HT

ポート参照

ファイアウォール アプリケーション インスペクション ガイド

ASA シリーズ参考情報

http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html

PIX アプリケーション Inspection Configuration Guides

http://www.cisco.com/c/en/us/support/security/pix-firewall-software/products-installation-and-configuration-guides-list.html

『FWSM 3.1 Application Inspection Configuration Guide』

http://www-author.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/inspct_f.html

IETF TCP/UDP ポート割り当てリスト

インターネット割り当て番号局（IANA）IETF 割り当てポート リスト

http://www.iana.org/assignments/port-numbers

IP テレフォニー設定とポート使用に関するガイド

『Cisco CRS 4.0 (IP IVR and IPCC Express) Port Utilization Guide』

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

『Port Utilization Guide for Cisco ICM/IPCC Enterprise and Hosted Editions』

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

Cisco Unified Communications Manager Express Security Guide to Best Practices

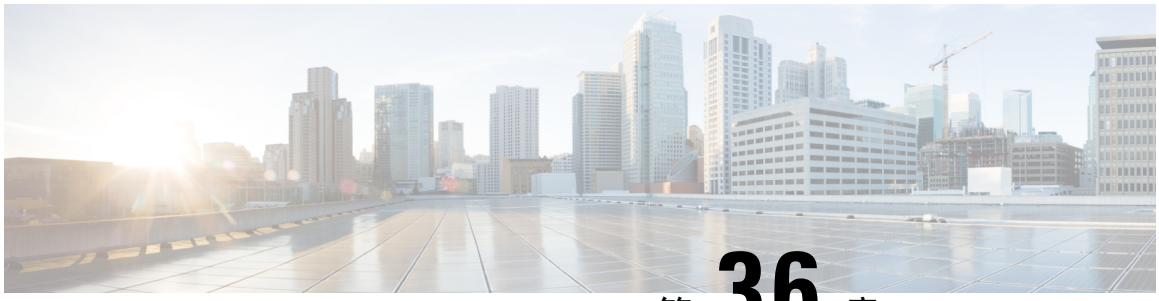
http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html

Cisco Unity Express Security Guide to Best Practices

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e31.html#wp41149

VMware ポート割り当てリスト

vCenter Server、ESX ホスト、およびその他のネットワーク コンポーネントの管理アクセス用の TCP ポートおよび UDP ポート



第 36 章

IM and Presence Service のポート使用状況の情報

IM and Presence Service ポート利用の概要

このマニュアルには、 IM and Presence Service が、クラスタ内接続用および、外部アプリケーションまたは外部デバイスとの通信用に使用する TCP および UDP ポートの一覧を示します。これは、IP Communications ソリューションの実装時に、ネットワークにファイアウォール、アクセス制御リスト（ACL）、および Quality of Service（QoS）を設定するうえで重要な情報となります。

（注） シスコでは、これらのポートで想定されるすべての設定シナリオを検証しているわけではありません。この一覧を参考にした結果、設定に問題が発生した場合は、シスコのテクニカルサポートにお問い合わせください。

事実上すべてのプロトコルが双方向で行われますが、このマニュアルではセッション開始側から見た方向を記載しています。デフォルトのポート番号は、管理者が手動で変更できる場合もありますが、ベスト プラクティスとしてこのような変更は推奨しません。IM and Presence Serviceは、内部使用に限定していくつかのポートを開くことに留意してください。

このドキュメントのポートは、IM and Presence サービスに特別に適用されます。リリースによってポートが異なる場合があり、今後のリリースで新しくポートが追加される可能性もあります。このため、参照しているマニュアルのバージョンが、インストールされている IM and Presence Service のバージョンと一致していることを確認してください。

ファイアウォール、ACL、または QoS の設定内容は、トポロジ、ネットワーク セキュリティ デバイスの配置に対するデバイスとサービスの配置、および使用するアプリケーションとテレフォニー拡張機能の種類に応じて異なります。また、デバイスやバージョンによって、ACL のフォーマットが異なることにも注意してください。

表に記載の情報

この表は、このマニュアルの表で確認できる情報を示します。

表 *62 :* 表の内容

表の項目	説明
From	ポートに要求を送信するクライアント
送信先	ポートで要求を受信するクライアント
ロール	クライアントまたはサーバのアプリケーションまたはプロセス
プロトコル	通信の確立と終了に使用されるセッション層プロトコル、またはトランザクションの要求と応答に使用されるアプリケーション層プロトコルのどちらか。
トランスポートプロトコル	コネクション型（TCP）またはコネクションレス型（UDP）のトランスポート層プロトコル
宛先/リスナー	要求の受信に使用されるポート
ソース/送信元	要求の送信に使用されるポート

IM and Presence サービス ポート リスト

次のテーブルは、IM and Presence サービスがクラスタ内とクラスタ間のトラフィックに使用するポートを示します。

表 *63 : IM and Presence* サービス ポート：*SIP* プロキシの要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
SIP ゲートウェイ --- IM and Presence	IM and Presence --- SIP ゲートウェイ	SIP	TCP/UDP	[5060]	エフェメラル	デフォルトの SIP プロキシの UDP および TCP リスナー
SIP ゲートウェイ	IM and Presence	SIP	TLS	5061	エフェメラル	TLS サーバー認証のリスナー ポート

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	IM and Presence	SIP	TLS	5062	エフェメラル	TLS 相互認証のリスナー ポート
IM and Presence	IM and Presence	SIP	UDP/TCP	5049	エフェメラル	内部ポート。ローカルホスト トラフィック専用。
IM and Presence	IM and Presence	HTTP	TCP	8081	エフェメラル	設定の変更を示す設定のエージェントからの HTTP 要求に使用されます。
サードパーティ製クライアント	IM and Presence	HTTP	TCP	8082	エフェメラル	デフォルトの IM and Presence HTTPのリスナー。サードパーティ製クライアントからの接続に使用されます。
サードパーティ製クライアント	IM and Presence	HTTPS	TLS/TCP	8083	エフェメラル	デフォルトの IM and Presence HTTPS リスナー。サードパーティ製クライアントからの接続に使用されます。

表 *64 : IM and Presence* サービス ポート：*Presence* エンジンの要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	IM and Presence（Presence エンジン）	SIP	UDP/TCP	5080	エフェメラル	デフォルトの SIP UDP/TCP リスナー ポート
IM and Presence（Presence エンジン）	IM and Presence（Presence エンジン）	Livebus	UDP	50000	エフェメラル	内部ポート。ローカルホスト トラフィック専用。LiveBus メッセージング ポート。IM and Presence サービスは、クラスタ通信に対してこのポートを使用します。

表 *65 : IM and Presence* サービス ポート：シスコの *Tomcat WebRequests*

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
ブラウザ	IM and Presence	HTTPS	TCP	8080	エフェメラル	ウェブアクセスに使用されます。
ブラウザ	IM and Presence	AXL/HTTPS	TLS/TCP	8443	エフェメラル	SOAP によりデータベースおよびサービスアビリティへのアクセスを提供します。
ブラウザ	IM and Presence	HTTPS	TLS/TCP	8443	エフェメラル	Web 管理へのアクセスを提供します。
ブラウザ	IM and Presence	HTTPS	TLS/TCP	8443	エフェメラル	ユーザー オプション ページへのアクセスを提供します。
ブラウザ	IM and Presence	SOAP	TLS/TCP	8443	エフェメラル	SOAP により Cisco Unified Personal Communicator、Cisco Unified Mobility Advantage、およびサードパーティ製の API クライアントへのアクセスを提供します。
ブラウザ	IM and Presence	HTTPS	TCP	9463	エフェメラル	Hypertext Transport Protocol over SSL（HTTPS）では、TLS1.3 の v6 のみが使用可能です。

表 *66 : IM and Presence* サービス ポート：外部社内ディレクトリ要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence ---------- 外部企業ディレクトリ	外部企業ディレクトリ ---------- IM and Presence	LDAP	TCP	389 / 3268	エフェメラル	ディレクトリプロトコルを外部企業ディレクトリと統合できるようにします。この LDAP ポートは、統合される社内ディレクトリによって異なります（デフォルトは 389）。Netscape Directory の場合は、別のポートで LDAP トラフィックを受信するよう設定できます。 認証用に IM&P と LDAP サーバー間の通信を LDAP に許可します。
IM and Presence	外部企業ディレクトリ	LDAPS	TCP	636	エフェメラル	ディレクトリプロトコルを外部企業ディレクトリと統合できるようにします。この LDAP ポートは、統合される社内ディレクトリによって異なります（デフォルトは 636）。

表 *67 : IM and Presence* サービス ポート：リクエストの設定

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（設定エージェント）	IM and Presence（設定エージェント）	TCP	[TCP]	8600	エフェメラル	設定エージェントのハートビート ポート

表 *68 : IM and Presence* サービス ポート：*Certificate Manager* の要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	証明書マネージャ	TCP	[TCP]	7070	エフェメラル	内部ポート。ローカルホストトラフィック専用。

表 *69 : IM and Presence* サービス ポート：*IDS*データベースの要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（データベース）	IM and Presence（データベース）	TCP	[TCP]	1500	エフェメラル	データベースクライアント用の内部 IDS ポート。ローカルホストトラフィック専用。
IM and Presence（データベース）	IM and Presence（データベース）	TCP	[TCP]	1501	エフェメラル	内部ポート：アップグレード中に IDS の 2 次インスタンスを始動するための代替ポートです。ローカルホストトラフィック専用。
IM and Presence（データベース）	IM and Presence（データベース）	XML	TCP	1515	エフェメラル	内部ポート。ローカルホストトラフィック専用。DB レプリケーション ポート。

表 *70 : IM and Presence Service* ポート：*IPSec* マネージャの要求

送信元 送信者	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（IPSec）	IM and Presence（IPSec）	専用	UDP/TCP	8500	8500	内部ポート：ipsec_mgr デーモンがプラットフォーム データ（ホスト）の証明書のクラスタレプリケーションに使用するクラスタ マネージャ ポートです。

表 *71 : IM and Presence* サービス ポート：*DRF*にマスター エージェント サーバー要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（DRF）	IM and Presence（DRF）	TCP	[TCP]	4040	エフェメラル	DRF Master Agent サーバー ポート。Local Agent、GUI、および CLI からの接続を受け入れます。

表 *72 : IM and Presence* サービス ポート：*RISDC* 要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（RIS）	IM and Presence（RIS）	TCP	[TCP]	2555	エフェメラル	Real-time Information Services（RIS）データベース サーバー。クラスタの 別の RISDC に接続し、クラスタ全体のリアルタイム情報を提供します。
IM and Presence（RTMT/AMC/SOAP）	IM and Presence（RIS）	TCP	[TCP]	2556	エフェメラル	Cisco RIS 向け Real-time Information Services（RIS）データベース クライアント。RIS クライアント接続で、リアルタイム情報を取得できるようにする
IM and Presence（RIS）	IM and Presence（RIS）	TCP	[TCP]	8889	8888	内部ポート。ローカル ホスト トラフィック専用。サービス ステータスの要求および応答用として、RISDC（システム アクセス）が TCP で servM にリンクするために使用します。

表 *73 : IM and Presence* サービス ポート：*SNMP* の要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
SNMP サーバー	IM and Presence	SNMP	UDP	161、8161	エフェメラル	SNMP ベースの管理アプリケーションにサービスを提供
IM and Presence	IM and Presence	SNMP	UDP	6162	エフェメラル	SNMP マスター エージェントから転送される要求を受信するネイティブ SNMP エージェント。
IM and Presence	IM and Presence	SNMP	UDP	6161	エフェメラル	ネイティブ SNMP エージェントからのトラップ情報を受信し、管理アプリケーションに転送する SNMP マスター エージェント。
SNMP サーバー	IM and Presence	TCP	[TCP]	7999	エフェメラル	CDP Agent が CDP バイナリと通信するためにソケットとして使用します。
IM and Presence	IM and Presence	TCP	[TCP]	7161	エフェメラル	SNMP マスターエージェントとサブエージェント間の通信に使用されます。
IM and Presence	SNMP トラップ モニター	SNMP	UDP	162	エフェメラル	SNMP トラップを管理アプリケーションに送信します。
IM and Presence	IM and Presence	SNMP	UDP	設定可能	61441	内部 SNMP トラップ レシーバ

表 *74 : IM and Presence* サービス ポート：*Racoon* サーバー要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
ゲートウェイ ---------- IM and Presence	IM and Presence ---------- ゲートウェイ	Ipsec	UDP	500	エフェメラル	Internet Security Association と KeyManagement Protocol を有効化

表 *75 : IM and Presence* サービス ポート：システム サービス要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（RIS）	IM and Presence（RIS）	XML	TCP	8888 および 8889	エフェメラル	内部ポート。ローカル ホスト トラフィック専用。RIS サービス マネージャ（servM）と通信するクライアントを受信するために使用します。

表 *76 : IM and Presence* サービス ポート：*DNS* 要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	DNS サーバー	DNS	UDP	53	エフェメラル	DNS サーバーが IM and Presence DNS 照会を受信するポート。 宛先:DNS サーバー|送信元:IM and Presence

表 *77 : IM and Presence* サービス ポート：*SSH/SFTP* 要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	エンドポイント	SSH/SFTP	TCP	22	エフェメラル	多くのアプリケーションが、サーバーへのコマンドラインアクセスを行うために使用します。ノード間で証明書などのファイル交換（sftp）にも使用されます。

表 *78 : IM and Presence* サービス ポート：*ICMP* 要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence ---------- Cisco Unified Communications Manager	Cisco Unified Communications Manager ---------- IM and Presence	ICMP	IP	N/A	エフェメラル	インターネット制御メッセージプロトコル（ICMP）。Cisco Unified Communications Manager サーバーとの通信に使用されます。

表 *79 : IM and Presence* サービス ポート：*NTP* 要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	NTP サーバー	NTP	UDP	123	エフェメラル	Cisco Unified Communications Manager は NTP サーバーとして動作します。サブスクライバノードが、パブリッシャノードと時刻を同期するために使用されます。

表 *80 : IM and Presence* サービス ポート：*Microsoft Exchange* 通知要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
Microsoft Exchange	IM and Presence	HTTP（HTTPu）	) WebDAV：HTTP /UDP/IP 通知 2) EWS - HTTP/TCP/IP SOAP 通知	IM and Presence サーバー ポート（デフォルト 50020）	エフェメラル	Microsoft Exchange は、このポートを使用してカレンダーイベントの特定のサブスクリプション識別子に対する変更を示す通知（NOTIFY メッセージによって示される）を送信します。ネットワーク構成内にある Exchange サーバーと統合する場合に使用されます。どちらのポートも作成されます。送信されるメッセージの種類は、設定するカレンダー プレゼンス バックエンドゲートウェイのタイプによって異なります。

表 *81 : IM and Presence* サービス ポート：*SOAP* サービス リクエスト

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（Tomcat）	IM and Presence（SOAP）	TCP	[TCP]	5007	エフェメラル	SOAP モニター ポート

表 *82 : IM and Presence* サービス ポート：*AMC RMI* 要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	RTMT	TCP	[TCP]	1090	エフェメラル	AMC RMI オブジェクト ポートRTMT パフォーマンス モニター、データ収集、ロギング、およびアラート生成用の Cisco AMC サービス。
IM and Presence	RTMT	TCP	[TCP]	1099	エフェメラル	AMC RMI レジストリ ポートRTMT パフォーマンス モニター、データ収集、ロギング、およびアラート生成用の Cisco AMC サービス。

表 *83 : IM and Presence* サービス ポート：*XCP* 要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
XMPP クライアント	IM and Presence	TCP	[TCP]	5222	エフェメラル	クライアント アクセス ポート
IM and Presence	IM and Presence	TCP	[TCP]	5269	エフェメラル	サーバー間接続（S2S）ポート
サードパーティ製 BOSH クライアント	IM and Presence	TCP	[TCP]	7335	エフェメラル	XCP Web Connection Manager が、BOSH を使用するサードパーティ製 API との接続に使用する HTTP リスニング ポート

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（XCP サービス）	IM and Presence（XCP ルータ	TCP	[TCP]	7400	エフェメラル	XCP ルータ マスター アクセス ポート。オープン ポート設定からルータに接続する XCP サービス（XCP 認証コンポーネント サービスなど）は、通常このポートを使用して接続します。
IM and Presence（XCP ルータ	IM and Presence（XCP ルータ	UDP	UDP	5353	エフェメラル	MDNS ポート。クラスタ内の XCP ルータはこのポートを使用してお互いを検出します。
IM and Presence（XCP ルータ	IM and Presence（XCP ルータ	TCP	[TCP]	7336	HTTPS	MFT ファイル転送（オンプレミスのみ）。

表 *84 : IM and Presence* サービスポート ― 外部データベースリクエスト

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	PostgreSQL データベース	TCP	[TCP]	5432 [1]	エフェメラル	PostgreSQL データベース リスニング ポート
IM and Presence	Oracle データベース	TCP	[TCP]	1521	エフェメラル	Oracle データベース リスニング ポート
IM and Presence	MSSQL データベース	TCP	[TCP]	1433	エフェメラル	MSSQL データベース リスニング ポート

[1] これがデフォルトのポートですが、任意のポートで受信するよう PostgreSQL データベースを設定できます。

表 *85 : IM and Presence* サービス ポート：高可用性の要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（Server Recovery Manager）	IM and Presence（Server Recovery Manager）	TCP	[TCP]	20075	エフェメラル	Cisco Server Recovery Manager が管理 RPC リクエストを行うために使用するポート。
IM and Presence（Server Recovery Manager）	IM and Presence（Server Recovery Manager）	UDP	UDP	21999	エフェメラル	Cisco Server Recovery Manager がピアとの通信に使用するポート。

表 *86 : IM and Presence* サービス ポート：*In Memory* データベース レプリケーションのメッセージ

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	IM and Presence	専用	TCP	6603*	エフェメラル	Cisco Presence Datastore
IM and Presence	IM and Presence	専用	TCP	6604*	エフェメラル	Cisco Login Datastore
IM and Presence	IM and Presence	専用	TCP	6605*	エフェメラル	Cisco SIP Registration Datastore
IM and Presence	IM and Presence	専用	TCP	9003	エフェメラル	Cisco Presence Datastore デュアル ノード プレゼンス冗長グループの複製。
IM and Presence	IM and Presence	専用	TCP	9004	エフェメラル	Cisco Login Datastore デュアル ノード プレゼンス冗長グループの複製。
IM and Presence	IM and Presence	専用	TCP	9005	エフェメラル	Cisco SIP Registration Datastore デュアル ノード プレゼンス冗長グループの複製。

* 管理 CLI 診断ユーティリティを実行するには、`utils imdb_replication status` コマンドを使用します。これらのポートは、クラスタの IM and Presence Service ノード間で設定されているすべてのファイアウォールでオープンである必要があります。このセットアップは、通常の運用では必要ありません。

表 *87 : IM and Presence* サービス ポート：*In Memory* データベース *SQL* メッセージ

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	IM and Presence	専用	TCP	6603	エフェメラル	Cisco Presence Datastore SQL クエリ。
IM and Presence	IM and Presence	専用	TCP	6604	エフェメラル	Cisco Login Datastore SQL クエリ。
IM and Presence	IM and Presence	専用	TCP	6605	エフェメラル	Cisco SIP Registration Datastore SQL クエリ。
IM and Presence	IM and Presence	専用	TCP	6606	エフェメラル	Cisco Route Datastore SQL クエリ。

表 *88 : IM and Presence* サービス ポート：*In Memory* データベースの通知メッセージ

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence	IM and Presence	専用	TCP	6607	エフェメラル	Cisco Presence Datastore XML ベースの変更通知。
IM and Presence	IM and Presence	専用	TCP	6608	エフェメラル	Cisco Login Datastore XML ベースの変更通知。
IM and Presence	IM and Presence	専用	TCP	6609	エフェメラル	Cisco SIP Registration Datastore XML ベースの変更通知。
IM and Presence	IM and Presence	専用	TCP	6610	エフェメラル	Cisco Route Datastore XML ベースの変更通知。

表 *89 : IM and Presence Service* ポート *:* 強制手動同期*/X.509* 証明書更新要求

送信元（送信者）	送信先（リスナー）	[プロトコル（Protocol）]	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence（Intercluster Sync Agent）	IM and Presence（Intercluster Sync Agent）	TCP	[TCP]	37239	エフェメラル	Cisco Intercluster Sync Agent サービスは、このポートを使用してコマンドを処理するためのソケット接続を確立します。

表 *90 : IM and Presence* サービス ポート：*ICMP* 要求

送信元（送信者）	送信先（リスナー）	宛先ポート	目的
エンドポイント/IM and Presence	IM and Presence	7	Internet Control Mess Protocol（ICMP）。トコル番号がエコーラフィックを伝送し見出しに示すようなるものではありま
IM and Presence	エンドポイント/IM and Presence		

表 *91 : IM and Presence* に使用するポート *- Cisco Unified CM* 通信および *IM and Presence Publisher - Subscriber* 通信

送信元（送信者）	送信先（リスナー）	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
Cisco Unified Communications Manager	IM and Presence Publisher	[TCP]	1500	双方向	データベースクライアント用内部 ID ポート。ローカルホスト トラフィック専用。
Cisco Unified Communications Manager	IM and Presence Publisher	[TCP]	8443	双方向	Web 管理へのアクセスを提供します。
Cisco Unified Communications Manager	IM and Presence Publisher	[TCP]	1090	双方向	AMC RMI オブジェクト ポートRTMT パフォーマンス モニター、データ収集、ロギング、およびアラート生成用の Cisco AMC サービス。

送信元（送信者）	送信先（リスナー）	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
Cisco Unified Communications Manager	IM and Presence Publisher	[TCP]	2555	双方向	双方向 Real-time Information Services（RIS）データベースサーバークラスタの 別の RISDC に接続し、クラスタ全体のリアルタイム情報を提供します。
Cisco Unified Communications Manager	IM and Presence Publisher	[TCP]	8500	双方向	内部ポート ー プラットフォームデータ（ホスト）証明書のクラスタレプリケーションに対して ipsec_mgr デーモンが使用するクラスタ管理ポート。
Cisco Unified Communications Manager	IM and Presence Publisher	[TCP]	8600	双方向	設定エージェントのハートビート ポート
Cisco Unified Communications Manager	IM and Presence Publisher	UDP	123	双方向	同期に使用する Network Time Protocol（NTP）。
IM and Presence Publisher	IM and Presence Subscriber	UDP	50000	双方向	内部ポート。ローカルホスト トラフィック専用。LiveBus メッセージング ポート。IM and Presence サービスは、クラスタ通信に対してこのポートを使用します。
IM and Presence Publisher	IM and Presence Subscriber	UDP	21999	双方向	Cisco Server Recovery Manager がピアとの通信に使用するポート。
IM and Presence Publisher	Cisco Unified Communications Manager	[TCP]	4040	双方向	DRF Master Agent サーバー ポート。Local Agent、GUI、および CLI からの接続を受け入れます。
IM and Presence Publisher	Cisco Unified Communications Manager	[TCP]	8001	双方向	常設チャットの構成中に使用されます。

送信元（送信者）	送信先（リスナー）	トランスポート プロトコル	宛先/リスナー	ソース/送信元	備考
IM and Presence Publisher	Cisco Unified Communications Manager	[TCP]	6379	双方向	マネージド ファイル転送（MFT）の構成中に使用されます。
IM and Presence Publisher	IM and Presence Subscriber	[TCP]	7	双方向	外部データベース（MSSQL）の構成中に使用されます。
IM and Presence Publisher	IM and Presence Subscriber	[TCP]	20075	双方向	Cisco Server Recovery Manager が管理 RPC リクエストを行うために使用するポート。
IM and Presence Publisher	IM and Presence Subscriber	[TCP]	8600	双方向	設定エージェントのハートビート ポート
IM and Presence Subscriber	IM and Presence Publisher	[TCP]	9005	双方向	Cisco SIP Registration Datastore デュアル ノード プレゼンス冗長グループの複製。
IM and Presence Subscriber	IM and Presence Publisher	[TCP]	9003	双方向	Cisco Presence Datastore デュアル ノードプレゼンス冗長グループの複製。
IM and Presence Subscriber	IM and Presence Publisher	[TCP]	20075	双方向	Cisco Server Recovery Manager が管理 RPC リクエストを行うために使用するポート。
IM and Presence Subscriber	IM and Presence Publisher	[TCP]	9004	双方向	Cisco Login Datastoreデュアル ノードプレゼンス冗長グループの複製。
Cisco Unified Communications Manager	IM and Presence Publisher	[TCP]	5070	双方向	コール構成で使用
IM and Presence Publisher	IM and Presence Subscriber	[TCP]	44000	双方向	コール構成で使用

表 *92 : On-a-call_Presence*

送信元（送信者）	送信先（リスナー）	送信元ポート	宛先ポート	プロトコル	備考
Cisco Unified Communications Manager	IM and Presence Publisher	[37240 – 61000]	5070	TCP	
IM and Presence Publisher	XMPP クライアント（Jabber）	5222	64846	[TCP]	クライアント アクセス ポート
IM and Presence Publisher	XMPP クライアント（Jabber）	5222	56361	[TCP]	クライアント アクセス ポート

表 *93 : MS-SQL DB* 構成

送信元（送信者）	送信先（リスナー）	送信元ポート	宛先ポート	プロトコル
IM and Presence Publisher	データベース	[37240 – 61000]	7	TCP

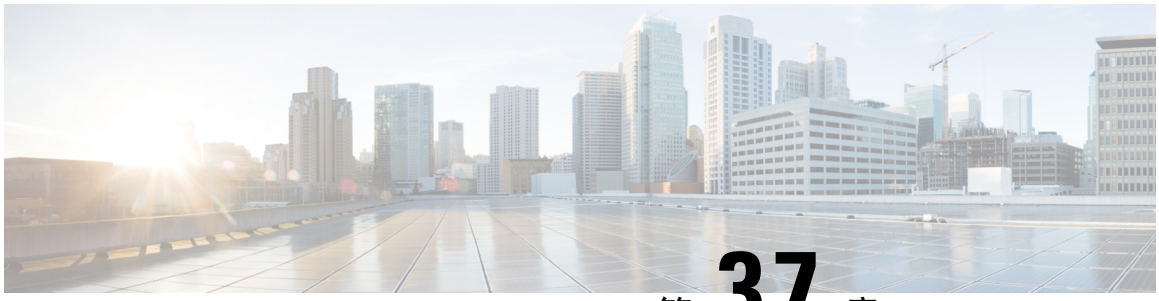
表 *94 : MS-SQL* 持続チャット構成

送信元（送信者）	送信先（リスナー）	送信元ポート	宛先ポート	プロトコル
IM and Presence Publisher	データベース	37240 – 61000	1433	[TCP]

表 *95 :* マネージド ファイル転送（*MFT*）構成

送信元（送信者）	送信先（リスナー）	送信元ポート	宛先ポート	プロトコル
IM and Presence Publisher	外部ファイルサーバ	37240 – 61000	7	TCP
IM and Presence Publisher	外部ファイルサーバ	37240 – 61000	22	TCP
IM and Presence Publisher	外部ファイルサーバ	37240 – 61000	5432	TCP
IM and Presence Publisher	データベース	54288 - 54292	5432	TCP

SNMP については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。



第 37 章

追加の要件

ハイ アベイラビリティ ログイン プロファイル

ハイ アベイラビリティ ログイン プロファイルに関する重要事項

- この項のハイ アベイラビリティ ログイン プロファイル テーブルを使用して、プレゼンス冗長グループのクライアント再ログインの上限値と下限値を設定できます。**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [サービス パラメータ（Service Parameters）]** を選択し、[サービス（Service）] メニューから [Cisco Server Recovery Manager] を選択して、クライアント ログインの上限値と下限値を設定します。
- ハイ アベイラビリティ クライアント ログイン プロファイルは、単一クラスタの展開でのみ適用されます。複数のクラスタが存在する場合、ハイ アベイラビリティ クライアント ログイン プロファイルには、冗長グループの上位および下位のクライアントの再ログイン値を設定することはできません。複数のクラスタ展開でハイ アベイラビリティ クライアント ログイン プロファイルを検出するには、さらにテストを実行する必要があります。
- Cisco XCP ルータサービスに対してデバッグロギングが有効になっている場合は、IM and Presence サービスに対して現在サポートされているロギングレベルの CPU 使用率の増加と減少が予想されます。
- ここに示すテーブルに基づいてプレゼンス冗長グループのクライアント再ログインの上限と下限を設定することで、展開のパフォーマンスの問題および高 CPU スパイクを回避できます。

- 各 IM and Presence Service ノードのメモリ サイズおよび各ハイ アベイラビリティ展開タイプ（アクティブ/アクティブまたはアクティブ/スタンバイ）用にハイ アベイラビリティ ログイン プロファイルを提供します。
- ハイ アベイラビリティ ログイン プロファイル テーブルは、次の入力に基づいて計算されます。
  - クライアント再ログインの下限は、Server Recovery Manager のサービス パラメータ「重要なサービス停止遅延（Critical Service Down Delay）」に基づいており、デフォルトは 90 秒です。重要なサービス停止遅延（Critical Service Down Delay）が変更されると、下限も必ず変わります。
  - アクティブ/スタンバイ展開のプレゼンス冗長グループ内のユーザ合計数、またはアクティブ/アクティブ展開のユーザが最も多いノード。
- プレゼンス冗長グループ内の両方のノードで、クライアント再ログインの上限値と下限値を設定する必要があります。プレゼンス冗長グループの両方のノードでこれらの値をすべて手動で設定する必要があります。
- クライアント再ログインの上限値と下限値は、プレゼンス冗長グループの各ノードで同じである必要があります。
- ユーザを**再平衡化**する場合は、ハイ アベイラビリティ ログイン プロファイル テーブルに基づくクライアント再ログインの上限値と下限値を再設定する必要があります。

ハイ アベイラビリティ ログイン プロファイル テーブルの使用

ハイ アベイラビリティ ログイン プロファイル テーブルを使用して、次の値を取得します。

- [クライアント再ログインの下限（Client Re-Login Lower Limit）] サービス パラメータ値
- [クライアント再ログインの上限（Client Re-Login Upper Limit）] サービス パラメータ値

手順

Step 1 仮想ハードウェア設定およびハイ アベイラビリティ展開タイプに基づいてプロファイル テーブルを選択します。

Step 2 プロファイル テーブルで、展開内のユーザ数を選択します（最も近い値に切り上げ）。アクティブ/スタンバイ展開を使用している場合、ユーザが最も多いノードを使用します。

Step 3 プレゼンス冗長グループの [ユーザ数（Number of Users）] の値に基づいて、プロファイル テーブル内の対応する再試行の下限値と上限値を取得します。

Step 4 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [サービス パラメータ（Service Parameters）]** を選択し、[サービス（Service）] メニューから [Cisco Server Recovery Manager] を選択して、IM and Presence Service の再試行の下限値と上限値を設定します。

Step 5 **[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [サービス パラメータ（Service Parameters）]** を選択し、[サービス（Service）] メニューから [Cisco Server Recovery Manager] を選択して [重要なサービス停止（Critical Service Down Delay）] の値を確認します。デフォルト値は 90 秒です。再試行下限値はこの値に設定してください。

高可用性 ログイン設定の例

例 1：ユーザ数 15,000 のフル UC プロファイル - アクティブ/アクティブ展開

プレゼンス冗長グループ内のユーザが 3,000 人で、あるノードに 2,000 人、2 台目のノードに 1,000 人のユーザがいます。非平衡型のアクティブ/アクティブ展開の場合、シスコはユーザが最も多いノード（この場合は、2,000 人のユーザが割り当てられているノード）を使用することを推奨します。ユーザ数 15,000 のフル米国（4 vCPU 8 GB）アクティブ/アクティブ プロファイルを使用して、次の再試行の下限値と上限値を取得します。

アクティブ ユーザの予想数	再試行下限値	再試行上限値
2000	120	253

（注） 再試行上限値は、フェールオーバー発生後にすべてのクライアントがバックアップ ノードにログインするまでのおおよその時間（秒）です。

（注） 120 の下限値は、**[重要なサービス停止遅延（Critical Service Down Delay）]** サービス パラメータが 120 に設定されていることを前提としています。

例 2：ユーザ数 5000 のフル UC プロファイル - アクティブ/アクティブ展開

プレゼンス冗長グループ内の各ノードに 4,700 人のユーザがいます。シスコは、最も近い値に切り上げ、ユーザ数 5,000 のフル米国（4 vCPU 8 GB）アクティブ/アクティブ プロファイルを使用して、ユーザ数 5,000 に基づいて、再試行の下限値と上限値を取得することを推奨します。

アクティブ ユーザの予想数	再試行下限値	再試行上限値
5,000	120	953

単一クラスタ コンフィギュレーション

500 ユーザ フル UC（1vCPU 700MHz 2GB）のアクティブ/アクティブ プロファイル

表 *96 :* 標準展開（*500* ユーザ フル *UC* のアクティブ/アクティブ）のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	187
250	120	287

500 ユーザ フル UC（1vCPU 700MHz 2GB）のアクティブ/スタンバイ プロファイル

表 *97 :* 標準展開（*500* ユーザ フル *UC* のアクティブ/スタンバイ）のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	187
250	120	287
500	120	453

1000 ユーザ フル UC（1vCPU 1500MHz 2GB）のアクティブ/アクティブ プロファイル

表 *98 :* 標準展開（*1000* ユーザ フル *UC* のアクティブ/アクティブ）のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	153

アクティブ ユーザの予想数	再試行下限値	再試行上限値
250	120	203
500	120	287

1000 ユーザ フル UC（1vCPU 1500MHz 2GB）のアクティブ/スタンバイ プロファイル

表 *99 :* 標準展開（*1000* ユーザ フル *UC* のアクティブ/スタンバイ）のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	153
250	120	203
500	120	287
750	120	370
1000	120	453

2000 ユーザ フル UC（1vCPU 1500Mhz 4GB）のアクティブ/アクティブ プロファイル

表 *100 :* 標準展開（*2000* ユーザ フル *UC* のアクティブ/アクティブ）のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	153
500	120	287
1000	120	453

2000 ユーザ フル UC（1vCPU 1500Mhz 4GB）のアクティブ/スタンバイ プロファイル

表 *101* : 標準展開（*2000* ユーザ フル *UC* のアクティブ/スタンバイ）のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	153
250	120	203
500	120	287
750	120	370
1000	120	453
1250	120	537
1,500	120	620
1750	120	703
2000	120	787

5000 ユーザ フル UC（4 GB 2vCPU）のアクティブ/アクティブ プロファイル

表 *102* : 標準展開（*5000* ユーザ フル *UC* のアクティブ/アクティブ）のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	137
500	120	203
1000	120	287
1,500	120	370
2000	120	453
2500	120	537

5000 ユーザ フル UC（4 GB 2vCPU）のアクティブ/スタンバイ プロファイル

注目　5000 ユーザシステムで最大のクライアント ログイン スループットを実現するために、シスコでは、少なくとも 2.6 GHz の CPU クロック速度を推奨しています。

表 *103* : 標準展開（*5000* ユーザ フル *UC* のアクティブ/スタンバイ）のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	154
500	120	287
1000	120	453
1,500	120	620
2000	120	787
2500	120	953
3,000	120	1120
3500	120	1287
4000	120	1453
4500	120	1620
5,000	120	1787

15000 ユーザ フル UC（4 vCPU 8GB）のアクティブ/アクティブ プロファイル

注目　15000 ユーザ システムで最大のクライアント ログイン スループットを実現するために、シスコでは、少なくとも 2.5GHz の CPU クロック速度を推奨しています。

表 *104* : 標準展開（*15000* ユーザ フル *UC* のアクティブ/アクティブ）のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		

アクティブ ユーザの予想数	再試行下限値	再試行上限値
100	120	127
500	120	153
1000	120	187
1,500	120	220
2000	120	253
2,500	120	287
3,000	120	320
3500	120	353
4000	120	387
4500	120	420
5000	120	453
6000	120	520
7000	120	587
7500	120	620

15000 ユーザ フル UC（4 vCPU 8GB）のアクティブ/スタンバイ プロファイル

注目　15000 ユーザシステムで最大のクライアント ログイン スループットを実現するために、シスコでは、少なくとも 2.6GHz の CPU クロック速度を推奨しています。

表 *105 :* 標準展開（*15000* ユーザ フル *UC* のアクティブ/スタンバイ）のユーザ ログイン再試行制限

アクティブ ユーザの予想数	再試行下限値	再試行上限値
フル UC		
100	120	137
500	120	203
1000	120	287
1,500	120	370

アクティブ ユーザの予想数	再試行下限値	再試行上限値
2000	120	453
2,500	120	537
3,000	120	620
3500	120	703
4000	120	787
4500	120	870
5000	120	953
6000	120	1120
7000	120	1287
8000	120	1453
9000	120	1620
10,000	120	1787
11000	120	1953
12000	120	2120
13,000	120	2287
14000	120	2453
15000	120	2620

25000ユーザフルUC（6vCPU16GB）のアクティブ/アクティブプロファイル

注目 25000ユーザシステムで最大のクライアントログインスループットを実現するために、シスコでは、少なくとも2.8GHzのCPUクロック速度を推奨しています。

表 ***106*** *:* アクティブ/アクティブプロファイルのログインレート*: **9*** は ***45% CPU*** を使用します。

アクティブ ユーザの予想数	再試行下限値	再試行上限値
100	120	131
500	120	176

アクティブ ユーザの予想数	再試行下限値	再試行上限値
1000	120	231
1,500	120	287
2000	120	342
2,500	120	398
3,000	120	453
3500	120	509
4000	120	564
4500	120	620
5,000	120	676
6000	120	787
7000	120	898
7500	120	953
8000	120	1009
9000	120	1120
10,000	120	1231
11000	120	1342
12000	120	1453
12500	120	1509

25000ユーザフル UC (6 vCPU 16 GB) アクティブ/スタンバイプロファイル

注目 25000 ユーザシステムで最大のクライアント ログイン スループットを実現するために、シスコでは、少なくとも 2.6GHz の CPU クロック速度を推奨しています。

表 *107 :* アクティブ/スタンバイ プロファイルのログイン率：*16* ユーザが *80%* の *CPU* を使用

アクティブ ユーザの予想数	再試行下限値	再試行上限値
100	120	133
500	120	183

アクティブ ユーザの予想数	再試行下限値	再試行上限値
1000	120	245
1,500	120	308
2000	120	370
2,500	120	433
3,000	120	495
3500	120	558
4000	120	620
4500	120	683
5,000	120	745
6000	120	870
7000	120	995
8000	120	1058
9000	120	1120
10,000	120	1245
11000	120	1370
12000	120	1495
13,000	120	1620
14000	120	1870
15000	120	1995
16000	120	2120
17000	120	2245
18000	120	2370
19000	120	2495
20000	120	2620
21000	120	2745
22000	120	2870
23000	120	2995
24000	120	3120

アクティブ ユーザの予想数	再試行下限値	再試行上限値
25000	120	3245

XMPP 標準への準拠

IM and Presence サービスは次の XMPP 標準に準拠しています。

- RFC 3920 Extensible Messaging and Presence Protocol (XMPP): Core RFC 3921 Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence
  - XEP-0004 Data Forms
  - XEP-0012 Last Activity
  - XEP-0013 Flexible Offline Message Retrieval
  - XEP-0016 Privacy Lists
  - XEP-0030 Service Discovery
  - XEP-0045 Multi-User Chat
  - XEP-0054 Vcard-temp
  - XEP-0055 Jabber Search
  - XEP-0060 Publish-Subscribe
  - XEP-0065 SOCKS5 Bystreams
  - XEP-0066 Out of Band Data Archive OOB requests
  - XEP-0068 Field Standardization for Data Forms
  - XEP-0071 XHTML-IM
  - XEP-0082 XMPP Date and Time Profiles
  - XEP-0092 Software Version
  - XEP-0106 JID Escaping
  - XEP-0114 Jabber Component Protocol
  - XEP-0115 Entity Capabilities
  - XEP-0124 Bidirectional Streams over Synchronous HTTP (BOSH)
  - XEP-0126 Invisibility
  - XEP-0128 Service Discovery Extensions
  - XEP-0160 Best Practices for Handling Offline Messages
  - XEP-0163 Personal Eventing Via PubSub
  - XEP-0170 Recommended Order of Stream Feature Negotiation

- XEP-0178 Best Practices for Use of SASL EXTERNAL
- XEP-0220 Server Dialback
- XEP-0273 SIFT (Stanza Interception and Filtering Technology)

設定変更通知およびサービス再起動通知

サービスを再起動する必要がある場合は常に、**アクティブな通知**ポップアップが表示されます。Cisco Unified CM IM and Presence 管理 GUI ヘッダーの右上に、**アクティブな通知の概要**が表示されます。

さらに、Cisco Unified CM IM and Presence 管理インターフェイスから [**システム** > **通知(System notification)**] を選択して、アクティブな通知リストにアクセスすることもできます。

再起動が必要な設定変更

多くの IM and Presence 設定の変更と更新については、Cisco XCP ルータ、Cisco SIP プロキシ、または Cisco Presence エンジンを再起動する必要があります。

次の表に、これらのサービスの再起動が必要な設定変更を示します。このリストには設定の変更が含まれていますが、インストールやアップグレードなどのプラットフォームの変更は含まれていません。

再起動が必要な設定	再起動するサービス
アプリケーション リスナーの設定 （[システム（System）] > [アプリケーションリスナー（Application Listeners）]） アプリケーション リスナーの編集	Cisco SIP Proxy
コンプライアンス プロファイルの設定 (Messaging > コンプライアンス > コンプライアンス設定) (Messaging > コンプライアンス > コンプライアンスプロファイル サードパーティコンプライアンスサーバに割り当てられているイベントの設定を編集する場合	Cisco XCP Router
グループ チャットのシステム管理者 （[メッセージング（Messaging）] > [グループチャットのシステム管理者（Group Chat System Administrators）]） この設定を有効または無効にすると、	Cisco XCP Router

再起動が必要な設定	再起動するサービス
外部ファイル サーバの設定 （[メッセージング（Messaging）] > [外部サーバの設定（External Server Setup）] > [外部ファイルサーバ（External File Servers）]） [**ホスト/Ip アドレス (Host/IP Address)**] 設定を編集する場合 **外部ファイルサーバの公開キー**を再生成する場合	Cisco XCP Router
グループ チャットと持続チャットの設定 （[メッセージング（Messaging）] > [グループチャットと持続チャット（Group Chat and Persistent Chat）]） 起動時にチャットノードが外部データベースに到達できない場合は、Cisco XCP Text 会議マネージャサービスが実行されていません。	Cisco XCP Router
グループ チャット サーバ エイリアス マッピング （[メッセージング（Messaging）] > [グループチャットサーバエイリアスマッピング（Group Chat Server Alias Mapping）]） チャットエイリアスの追加	Cisco XCP Router
ACL 設定 （[システム（System）] > [セキュリティ（Security）] > [着信ACL（Incoming ACL）]） （[システム（System）] > [セキュリティ（Security）] > [発信ACL（Outgoing ACL）]） 着信または発信 ACL の設定の編集	Cisco SIP Proxy
コンプライアンス設定 メッセージアーカイバ: 設定を編集します。	Cisco XCP Router
LDAP サーバ（LDAP Server） (アプリケーション > サードパーティ製クライアント > サードパーティの LDAP 設定) LDAP 検索: LDAP 検索の編集 LDAP からのビルド Vcard の編集 VCard FN に使用する LDAP 属性の編集	Cisco XCP Router

再起動が必要な設定	再起動するサービス
メッセージ設定の構成 （[メッセージング（Messaging）] > [設定（Settings）]） [インスタントメッセージの有効化 (Enable instant message)] の編集 オフライン中の相手へのインスタントメッセージの送信を無効にする	Cisco XCP Router
プレゼンス ゲートウェイ（Presence Gateway） （[プレゼンス（Presence）] > [ゲートウェイ（Gateways）]） プレゼンス ゲートウェイの追加、編集、削除 MS Exchange 証明書をアップロードした後	Cisco Presence Engine
プレゼンス設定の構成 （[プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）]） [プレゼンスステータスの共有を有効にする（Enable Availability Sharing）] 設定の編集 確認プロンプトなしで、ユーザが他のユーザのプレゼンスステータスを表示できるようにする 連絡先リストの最大サイズ（ユーザごと）（Maximum Contact List Size (per user)） 最大数のウォッチャー	Cisco Presence Engine Cisco XCP Router
プレゼンス設定の構成 （[プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）]） [**Enable user Of Email address For ドメイン間フェデレーション**] フィールドの編集	Cisco XCP Router

再起動が必要な設定	再起動するサービス
パーティション イントラドメイン フェデレーションの設定 [プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）]（チェックボックス） プレゼンス > イントラドメインフェデレーションのセットアップ (ウィザード) チェックボックスを使用するか、またはウィザードを使用して、LC/OCS/Lync とのパーティションイントラドメインフェデレーションを有効にします。 パーティション分割されたイントラドメインルーティングモード: [Standard Configuration] ウィンドウまたはウィザードを使用して設定します。	これらの設定を編集すると、Cisco SIP プロキシが自動的に再起動します さらに、XCP ルータを再起動する必要があります。
プロキシ設定 （[プレゼンス（Presence）] > [ルーティング（Routing）] > [設定（Settings）]） プロキシ設定に対するすべての編集	Cisco SIP Proxy
セキュリティ設定（Security Settings） （[システム（System）] > [セキュリティ（Security）] > [設定（Settings）]） Sip クラスタ内プロキシからプロキシトランスポートプロトコルなどの SIP セキュリティ設定の編集 XMPP セキュリティ設定の編集	Cisco SIP プロキシ (SIP セキュリティの編集用) Cisco XCP ルータ (XCP セキュリティの編集用)
SIP フェデレーテッド ドメイン （[プレゼンス（Presence）]>[ドメイン間フェデレーション（Interdomain Federation）] > [SIPフェデレーション（SIP Federation）]） この設定の追加、編集、削除	Cisco XCP Router
サードパーティ製コンプライアンス サービス (アプリケーション > サードパーティ製クライアント > サードパーティ製 LDAP サーバ) [Hostname/IP Address]、[Port]、[Password]、[Confirm Password] の各フィールドを編集します。	Cisco XCP Router

再起動が必要な設定	再起動するサービス
TLS ピア サブジェクトの設定 （[システム（System）] > [セキュリティ（Security）] > [TLSピアサブジェクト（TLS Peer Subjects）]） このページでの編集	Cisco SIP Proxy
TLS コンテキスト （[システム（System）] > [セキュリティ（Security）] > [TLSコンテキスト設定（TLS Context Configuration）]） このページでのいずれかの編集	関連付けられているチャットサーバの再起動が必要になる場合があります
XMPP フェデレーション （[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）]） （[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）]） XMPP フェデレーションに対するすべての編集	Cisco XCP Router
クラスタ間ピアリング （プレゼンス クラスタ間設定） クラスタ間ピア設定の編集	場合によっては、Cisco XCP ルータを再起動するように求められる場合があります (右上のウィンドウに通知が表示されます)。
イーサネット設定 （[Cisco Unified IM and PresenceのOSの管理（Cisco Unified IM and Presence OS Administration）] から、[設定（Settings）] > [IP] > [イーサネット/イーサネットIPv6（Ethernet/Ethernet IPv6）]） いずれかのイーサネット設定の編集	システムがすぐに再起動される
IPv6 設定 （[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]） [IPv6を有効化] エンタープライズパラメータの有効化の編集	Cisco XCP Router Cisco SIP Proxy Cisco Presence Engine

再起動が必要な設定	再起動するサービス
トラブルシューティング サブスクライバがオフラインのときにIM and Presenceパブリッシャが変更された場合 サブスクライバから > IP > パブリッシャの設定を編集します。	サブスクライバノードの再起動
IM and Presenceのアップグレード中に、以前のバージョンに切り替える必要があります	システムを再起動します。
cup 証明書の再生成	Cisco SIP Proxy Cisco Presence Engine
カップの再生成-xmpp	Cisco XCP Router
cup-xmpp-s2s 証明書の再生成	Cisco XCP Router
新しい証明書のアップロード	その証明書に関連するサービスを再起動します。 カップ信頼証明書の場合は、Cisco SIP プロキシを再起動します。
リモート監査ログの転送プロトコル 任意のユーティリティ remotesyslog set protocol * CLI コマンドを実行する場合	ノードの再起動
次のいずれかのアラートが表示された場合: • PEIDSQueryError • PEIDStoIMDBDatabaseSyncError • PEIDSSubscribeError • PEWebDAVInitializationFailure	Cisco Presence エンジンを再起動することをお勧めします。
次のアラートのいずれかを受け取った場合 • • XCPConfigMgrJabberRestartRequired • XCPConfigMgrR2RPasswordEncryptionFailed • XCPConfigMgrR2RRequestTimedOut • XCPConfigMgrHostNameResolutionFailed	Cisco XCP ルータを再起動することをお勧めします。

再起動が必要な設定	再起動するサービス
PWSSCBInitFailed	Cisco SIP プロキシを再起動することをお勧めします。
Exchange サービスパラメータの編集 • Microsoft Exchange 通知ポート（Microsoft Exchange Notification Port） • カレンダーの拡散 • Exchange タイムアウト（秒）（Exchange Timeout (seconds)） • Exchange キュー（Exchange Queue） • スレッドの交換 • EWS ステータスの頻度	Cisco Presence Engine
Exchange 証明書のアップロード	Cisco SIP Proxy Cisco Presence Engine
ロケールのインストール	IM and Presence サービスの再起動
新しい MSSQL 外部データベースの作成	Cisco XCP Router
外部データベース設定の編集	Cisco XCP Router
外部データベースのマージ	Cisco XCP Router
TLS ピア サブジェクトの設定	Cisco SIP Proxy
ピア認証 TLS コンテキストの設定	Cisco SIP Proxy
次の Cisco SIP プロキシサービスパラメータを編集します。 • CUCM ドメイン • サーバ名 (補足) • HTTP ポート（HTTP Port） • ステートフルサーバ (トランザクションステートフル) • TCP 接続の永続化 • 共有メモリサイズ（バイト）（Shared memory size (bytes)） • フェデレーションルーティング IM/P FQDN • Microsoft フェデレーションのユーザエージェントヘッダー (カンマ区切り)	Cisco SIP Proxy

再起動が必要な設定	再起動するサービス
ルーティング通信タイプのサービスパラメータの編集	Cisco XCP Router
IM アドレススキームの編集	Cisco XCP Router
デフォルトドメインの割り当て	Cisco XCP Router
クラスタからのノードの削除または削除	Cisco XCP Router
Cisco XCP ルータに影響を与えるパラメータを編集するには、Cisco XCP ルータを再起動する必要があります。	Cisco XCP Router
ルーティング通信タイプサービスパラメータ	Cisco XCP Router
Cisco XCP File Transfer Manager サービスパラメータのいずれかを編集します。 • **外部ファイルサーバの使用可能なスペースの下限しきい値** • **外部ファイルサーバの使用可能領域の上限しきい値**	Cisco XCP Router
[マルチ**デバイスメッセージングの有効化 (Enable 複数 Device Messaging)**] サービスパラメータの編集	Cisco XCP Router
[**Maximum number of logon sessions per user**] サービスパラメータの編集	Cisco XCP Router
外部データベース上の`install_dir/data/pg_hba conf`または `install_dir/data/postgresql.conf` config ファイルの更新	Cisco XCP Router
移行ユーティリティ： • [プレゼンスの設定（Presence Settings）] ウィンドウでの [確認プロンプトなしで、ユーザが他のユーザのプレゼンスステータスを表示できるようにする（Allow users to view the availability of other users without being prompted for approval）] 設定の編集。 • [プレゼンス設定の構成 (プレゼンス設定の設定)] ウィンドウで、**連絡先リストの最大サイズ (ユーザ単位)**と**最大数のウォッチャー (ユーザごと)** の設定を編集します。	Cisco XCP Router
クラスタからのノードの削除または削除	Cisco XCP Router

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。