Cisco Unified Communications Manager Release 10.0(1) での IM and Presence Service の設定と管理

初版：2014 年 04 月 09 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 I 部

展開のプランニング

第 1 章

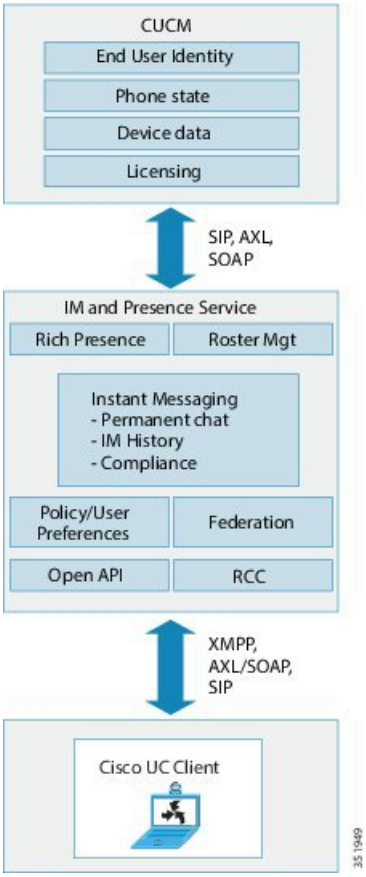
IM and Presence Service の機能

IM and Presence Service のコンポーネント

主要なコンポーネント

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 接続は、Cisco Unified Communications Manager と Cisco Unified Presence 間のプレゼンス情報交換を処理します。Cisco Unified Communications Manager の SIP 接続を有効にするには、Cisco Unified Presence サーバを指すように SIP トランクを設定する必要があります。

Cisco Unified Presence 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、Cisco Unified Presence は、SIP トランク経由で、SIP サブスクライブ メッセージを Cisco Unified Communications Manager に送信できます。

（注） Cisco Unified Presence は、TLS 経由で SIP/SIMPLE インターフェイスを使用することで Cisco Unified Presence に接続しているクライアント（シスコ クライアントまたはサードパーティ）をサポートしません。TCP 経由の SIP 接続だけがサポートされます。

関連トピック

Cisco Unified Communications Manager の SIP トランク設定, （60 ページ）
プレゼンス ゲートウェイの設定オプション, （97 ページ）

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化するには、IM and Presence Service で Sync Agent サービスを起動する必要があります。

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。また、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。

関連トピック

http://www.cisco.com/go/designzone

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。

関連トピック

LDAP ディレクトリ統合, （101 ページ）

LDAP サーバ名、アドレス、およびプロファイル設定, （101 ページ）
Cisco Unified Communications Manager と LDAP ディレクトリとの間のセキュア接続, （102 ページ）
XMPP クライアントの LDAP サーバの名前とアドレスの設定, （108 ページ）

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。

関連トピック

IM and Presence サービスと XMPP クライアント間のセキュア接続の設定, （138 ページ）

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。

CTI 機能は、Microsoft Office Communicator クライアントの IM and Presence Service リモート コール制御機能にも使用されます。リモート コール制御機能の設定については、「*Microsoft Office Communicator Call Control with Microsoft OCS for IM and Presence Service on Cisco Unified Communications Manager*」を参照してください。

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

Cisco IM and Presence Data Monitor は、IM and Presence Service の IDS の複製の状態を監視します。他の IM and Presence サービスは、IM and Presence Data Monitor に依存します。これらの依存サービスは、シスコのサービスを使用して、IDS の複製が安定した状態になるまで起動を遅らせます。

また、Cisco IM and Presence Data Monitor は Cisco Sync Agent の同期のステータスを Cisco Unified Communications Manager から確認します。依存サービスは、IDS の複製が設定され、IM and Presence データベース パブリッシャ ノードの Sync Agent が Cisco Unified Communications Manager からの同期を完了させた後にのみ、起動できます。タイムアウトになると、IDS の複製と Sync Agent が完

了していなくても、パブリッシャ ノードの Cisco IM and Presence Data Monitor は依存サービスの起動を許可します。

サブスクライバ ノードで、IDS の複製が正常に確立されるまで、Cisco IM and PresenceData Monitor は機能サービスの起動を遅らせます。Cisco IM and Presence Data Monitor のみがクラスタ内の問題のあるサブスクライバ ノードの機能サービスの起動を遅らせます。問題のある 1 個のノードのためにすべてのサブスクライバ ノードの機能サービスの起動を遅らせることはありません。たとえば、IDS の複製が node1 および node2 で正常に確立されたが、node3 では確立されない場合、Cisco IM and Presence Data Monitor により、機能サービスは node1 および node2 で開始できますが、node3 では機能サービスの開始が遅れます。

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。

- 次の CLI コマンドを使用します。

  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。

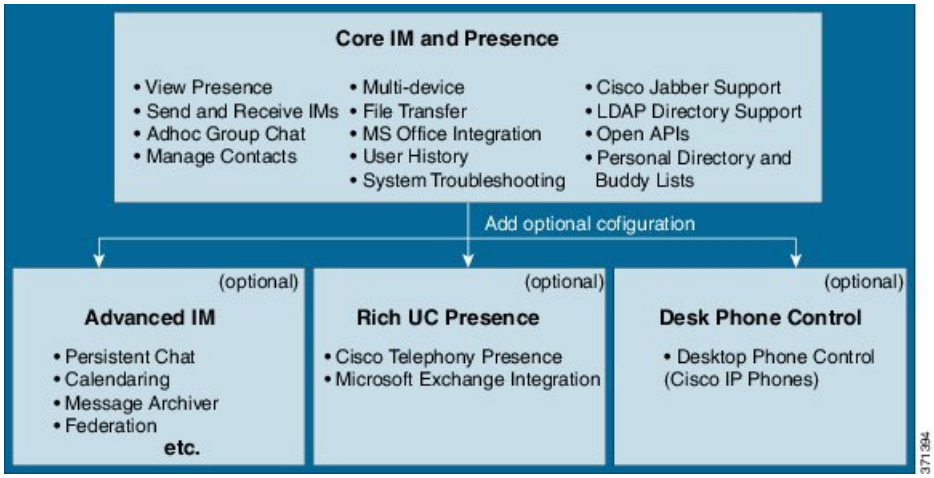
Cisco Sync Agent のステータスを確認するには、Cisco Unified CM IM and Presence の管理インターフェイスに移動し、[診断（Diagnostics）] > [システム ダッシュボード（System Dashboard）] を選択します。CUCM Publisher の IP アドレスと同期ステータスを検索します。

IM and Presence Service の機能展開オプション

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。

図 *2*：*IM and Presence Service* の機能展開オプション



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 *1*：*IM and Presence Service* の機能展開オプション

コア IM と可用性機能	高度な IM 機能（オプション）	豊富な Unified Communications 可用性機能（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 可用性の表示 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 テレフォニーの可用性 Microsoft Exchange サーバの統合	リモート Cisco IP Phone 制御 Microsoft Remote Call Control の統合

コア IM と可用性機能	高度な IM 機能（オプション）	豊富な Unified Communications 可用性機能（オプション）	リモート デスク フォン制御（オプション）
	永続的なチャット メッセージ アーカイバ カレンダー サードパーティ製 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 クラスタ間のピアリング 企業の連携（B2B）： • Cisco Unified Presence との統合 • Cisco WebEx の統合 • Mircosoft Lync/OCS サーバの統合（ドメイン間とパーティション化されたドメイン内のフェデレーション） • IBM SameTime の統合 • Cisco Jabber XCP パブリック フェデレーション（B2C）： • 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 シングル サインオン		

コア IM と可用性機能	高度な IM 機能（オプション）	豊富な Unified Communications 可用性機能（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		

配置モデル

IM-Only の展開

IM and Presence Service は IM-only 展開をサポートします。このタイプの展開では、ノードごとに最大 25,000 ユーザと IM and Presence Service クラスタに最大 75,000 ユーザがサポートされます。

関連トピック

IM-Only 展開のワークフロー, （53 ページ）

シングルノード、マルチノード、および IM-Only での高可用性展開

IM and Presence Service は、シングルノード、マルチノード、および IM-only での高可用性展開をサポートしています。

クラスタ内のシングルノード展開では、そのノードに割り当てられているユーザに対して、高可用性のフェールオーバー保護は提供されません。プレゼンス冗長グループを使用しているマルチノード展開では、グループに対して高可用性を有効にできるため、ユーザにはフェールオーバー保護が提供されます。

シスコでは、IM and Presence Service 展開を高可用性展開として設定することを推奨します。シングル展開では、高可用性と非高可用性の両方を、プレゼンス冗長グループに設定しておくことが許可されますが、この設定は推奨されません。プレゼンス冗長グループに対して、Cisco Unified CM Administration インターフェイスを使用して、高可用性を手動で有効にする必要があります。高可用性の設定方法の詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

すべての IM and Presence Service 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 Service ノード、またはペアの IM and Presence Service ノードで構成されている場合があります。高可用性には、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可用性 データベースとともに運用されます。

平衡型とアクティブ/スタンバイの 2 種類の異なる設定を使用することで、高可用性を実現できます。平衡型モードでは、連動するようにプレゼンス冗長グループ内のノードを設定できます。コンポーネントの障害や停電により、いずれかのノードが停止すると、ユーザのロード バランシングとユーザのフェールオーバーが自動的に有効になり、冗長高可用性が提供されます。アクティ

ブ/スタンバイの設定では、アクティブ ノードが停止すると、スタンバイ ノードはアクティブ ノードを自動的に引き継ぎます。

プレゼンス冗長グループ、高可用性 モード、およびユーザの割り当ての詳細や設定手順については、次のガイドを参照してください。

- 『*Cisco Unified Communications Manager Administration Guide*』
- 『*Cisco Unified Communications Manager Bulk Administration Guide*』
- 『*Cisco Unified Communications Manager Features and Services Guide*』
- 『*Cisco Unified Communications Manager Installation Guide*』
- 『*Cisco Unified Communications Manager System Guide*』

プレゼンス冗長グループと高可用性

プレゼンス冗長グループは、同じクラスタの 2 つの IM and Presence サービス ノードから構成され、IM and Presence サービスのクライアントとアプリケーションに冗長化とリカバリを提供します。[Cisco Unified CMの管理(Cisco Unified CM Administration)] を使用して、ノードをプレゼンス冗長グループに割り当て、高可用性を可能にします。

- 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（コマンド ライン インターフェイス）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。その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、回復したノードが使用可能になると、そのノードと再接続します。
  - 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 and Presence サービス ノードにフェールオーバーします。失敗したノードがオンラインに戻ると、クライアントはローカルの IM and Presence サービス ノードに自動的に再接続します。失敗したノードがオンラインに戻ったときに、自動フォールバック オプションを設定していない場合は、手動のフォールバック操作を行う必要があります。

プレゼンス冗長グループの IM and Presence サービス ノードのノード フェールオーバー、フォールバック、および回復は手動で開始できます。自動フォールバック オプションを設定していない場合は、手動のフォールバック操作を行う必要があります。

プレゼンス冗長グループおよび高可用性を設定する方法については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

WAN 経由のクラスタリング

IM and Presence Service は WAN 経由のクラスタリング展開をサポートします。

関連トピック

クラスタ内およびクラスタ間展開における WAN 経由のクラスタリング, （31 ページ）

ユーザ割り当て

ユーザが IM and Presence サービスの可用性と Instant Messaging（IM）サービスを受けられるようにするには、IM and Presence サービス展開でノードとプレゼンス冗長グループにユーザを割り当てる必要があります。IM and Presence 展開では、手動または自動でユーザを割り当てることができます。User Assignment Mode for Presence Server の [エンタープライズ パラメータ（Enterprise Parameter）] 設定を使用してユーザ割り当てを管理します。このパラメータは、Sync Agent がクラスタ内のノードにユーザを分散させるモードを指定します。

[平衡化（Balanced）] モード（デフォルト）では、ユーザをプレゼンス冗長グループの各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。デフォルト モードは [平衡化（Balanced）] です。

[アクティブ スタンバイ（Active-Standby）] モードでは、プレゼンス冗長グループ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 ノードをバックアップのままにします。

[なし（None）] 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。

手動のユーザ割り当てを選択した場合は、Cisco Unified Communications Manager Administration を使用してノードとプレゼンス冗長グループに手動でユーザを割り当てる必要があります。詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

エンド ユーザ管理

次のエンド ユーザの管理タスクを実行するには、IM and Presence Service GUI を使用できます。

- 重複しているか無効なエンド ユーザ インスタンスの有無を展開の全体にわたって確認します。
- 連絡先リストをエクスポートします。
- ホーム クラスタで連絡先リストをインポートします。

IM and Presence Service ユーザを移行する手順については、クラスタ間のユーザ移行、ユーザ管理、および管理に関するトピックを参照してください。

IM and Presence Service ノードへユーザを割り当てて、エンド ユーザを IM and Presence Service 用に設定する手順については、次のガイドを参照してください。

- 『*Cisco Unified Communications Manager Administration Guide*』
- 『*Cisco Unified Communications Manager Bulk Administration Guide*』
- 『*Installing Cisco Unified Communications Manager*』

可用性とインスタント メッセージ

チャット（Chat）

ポイントツーポイント インスタント メッセージ（IM）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。ユーザは、ポイントツーポイント IM を交換するために IM クライアントでオンラインである必要があります。

IM and Presence Service でチャットと可用性の両方の機能を無効にできます。

関連トピック

IM and Presence Service クラスタのインスタント メッセージのオン/オフ, （152 ページ）
IM and Presence サービス クラスタのプレゼンス ステータス共有のオン/オフ, （149 ページ）

IM 分岐

複数の IM クライアントにサイン インしている連絡先に、ユーザが IM を送信すると、IM and Presence Service は各クライアントに IM を配信します。この機能は、IM 分岐と呼ばれます。IM and Presence Service は、連絡先が応答するまで IM を各クライアントに分岐し続けます。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 メッセージは、IM and Presence Service で無効にできます。

関連トピック

オフライン インスタント メッセージのオン/オフ, （153 ページ）

オフライン IM

オフライン IM は、オフラインの連絡先に IM を送信する機能です。ユーザがオフラインの連絡先に IM を送信すると、IM and Presence Service は IM を保存し、オフラインの連絡先が IM クライアントにサイン インすると IM を配信します。

ブロードキャスト IM

ブロードキャスト IM は、同時に複数の連絡先に IM を送信する機能です。たとえば、ユーザは、連絡先の大きなグループに通知を送信できます。すべての IM クライアントがこの機能をサポートしているとは限りません。

IM and Presence Service のチャット ルーム

IM and Presence Service は、アドホック チャット ルームと永続的なチャット ルームの両方の IM 交換をサポートします。デフォルトで、IM and Presence Service の Text Conference（TC）コンポーネントは、アドホック チャット ルームの IM 交換を処理するように設定されています。このモジュールで説明するように、永続的なチャット ルームをサポートするには、追加要件の設定が必要になります。

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 IM セッションで、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。IM 会話のレコードは永続的に維持されません。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。ユーザは、招待されることによって参加できます。招待されない場合でも、サードパーティ製 XMPP クライアントでサービス検出またはルーム検索によってルームを見つけることにより参加できます。

永続的なチャット 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 セッションのように終了することはありません。その目的は、ユーザが後で永続的なチャット ルームに戻って、協力し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。管理者は、そのルームのメンバーだけがアクセスできるように永続的なチャット ルームへのアクセスを制限することもできます。メンバーの設定, （218 ページ）と、Cisco Unified Communications Manager および IM and Presence Service Release 11.0(1) のリリース ノートにある「Important Notes」セクションの「IM and Presence Service Ad Hoc Group Chat Rooms Privacy Policy」を参照してください。

IM and Presence Service の TC コンポーネントにより、ユーザは次の操作を実行できます。

- 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。
- ルームに他のユーザを招待します。
- ルームに表示されるメンバーのプレゼンス ステータスを確認します。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。

また、IM and Presence Service の永続的なチャット機能により、ユーザは次の操作を実行できます。

- 既存のチャット ルームを検索し、そのルームに入室します。
- チャットの音声テキスト変換を保存し、メッセージ履歴を検索できるようにします。

チャット ルームの制限

次の表に、IM and Presence Service のチャット ルームの制限値を示します。

表 *2*：*IM and Presence Service* のチャット ルームの制限

項目	最大数
ノードごとの永続的なチャット ルーム	1500 ルーム
ノードあたりのルームの合計（アドホックおよび永続的）	16500 ルーム
ルームごとの利用者	1000 利用者
アーカイブから取得されたメッセージ これは、ユーザがルーム履歴を問い合わせたときに返されるメッセージの最大数です。	100 メッセージ
デフォルトで表示されるチャット履歴のメッセージ これは、ユーザがチャット ルームに入室したときに表示されるメッセージの数です。	15 メッセージ

ファイル転送

IM and Presence Service は、XEP-0096（http://xmpp.org/extensions/xep-0096.html）に準拠した XMPP クライアント間のポイント ツー ポイント ファイル転送をサポートします。

関連トピック

ファイル転送の有効化, （205 ページ）

IM and Presence Service およびチャットに関する重要事項

SIP 間の IM では、次のサービスが 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 から XMPP への IM では、次のサービスが 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

IM コンプライアンス

IM and Presence Service におけるインスタント メッセージ（IM）のコンプライアンスの設定については、次のマニュアルを参照してください。

- 『*Instant Messaging Compliance Guide for IM and Presence Service on Cisco Unified Communications Manager*』

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

- 『*Database Setup Guide for IM and Presence Service on Cisco Unified Communications Manager*』

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

LDAP 統合

いくつかの異なる要件を満たすために、この統合に社内 LDAP ディレクトリを設定できます。

- **ユーザ プロビジョニング**：Cisco Unified Communications Manager データベースに LDAP ディレクトリからユーザを自動的にプロビジョニングできます。Cisco Unified Communications Manager は、LDAP ディレクトリの内容と同期するため、変更が LDAP ディレクトリで発生するたびにユーザ情報を手動で追加、削除、または修正する必要はありません。
- **ユーザ認証**：LDAP ディレクトリの資格情報を使用してユーザを認証できます。IM and Presence Service は Cisco Unified Communications Manager からすべてのユーザ情報を同期し、Cisco Jabber クライアントおよび IM and Presence Service ユーザ インターフェイスのユーザ認証を提供します。

シスコは、ユーザの同期化と認証のために、Cisco Unified Communications Manager と Directory サーバの統合を推奨しています。

（注） Cisco Unified Communications Manager を LDAP と統合しない場合は、IM and Presence Service を展開する前に、ユーザ名が Active Directory と Cisco Unified Communications Manager でまったく同じであることを確認する必要があります。

関連トピック

Cisco Unified Communications Manager との LDAP ディレクトリの統合のタスク リスト，（101 ページ）

サードパーティ統合

サードパーティ統合については、次の表の参照資料を参照してください。

マニュアルのタイトル	このマニュアルの構成
『Microsoft Exchange for IM and Presence Service on Cisco Unified Communications Manager』	• Microsoft Exchange 2003、2007、および 2010 との統合 • この統合のための Microsoft Active Directory の設定
『Microsoft Office Communicator Call Control with Microsoft OCS for IM and Presence Service on Cisco Unified Communications Manager』	• Microsoft Office Communicator クライアントからのリモート コール制御用 CSTA ゲートウェイとしての IM and Presence Service の設定 • この統合のための Microsoft Active Directory の設定 • TCP 経由のデュアル ノード IM and Presence Service 展開での MOC 要求のロード バランシング • TLS 経由のデュアル ノード IM and Presence Service 展開での MOC 要求のロード バランシング
『Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager』	• Microsoft OCS と AOL による SIP プロトコルを介したドメイン間フェデレーションと、IBM Sametime、Googletalk、Webex Connect、および別の IM and Presence Service Release 9.x エンタープライズによる XMPP プロトコルを介したドメイン間フェデレーション用の IM and Presence Service の設定。
『Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager』	• パーティション化されたドメイン内フェデレーション用の IM and Presence Service の設定 • パーティション化されたドメイン内フェデレーション用の Microsoft OCS の設定 • パーティション化されたドメイン内フェデレーション用の Microsoft LCS の設定 • ユーザの移行

マニュアルのタイトル	このマニュアルの構成
『Remote Call Control with Microsoft Lync Server for IM and Presence Service on Cisco Unified Communications Manager』	• Microsoft Lync と統合するための Cisco Unified Communications Manager および IM and Presence Service の設定 • Microsoft Active Directory の設定 • 正規化ルールの設定 • IM and Presence Service と Microsoft Lync 間のセキュリティの設定

サードパーティ製クライアントの統合

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、可用性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/

（注） サポートされるクライアントは、IM and Presence Service ノードに設定された IM アドレス スキームによって異なる場合があります。

サードパーティ製クライアントのライセンス要件

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。詳細については、『*Cisco Unified Communications Manager Enterprise License Manager User Guide*』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。

関連トピック

ユーザ ライセンスの要件, （41 ページ）
統合前の Cisco Unified Communications Manager のユーザおよびデバイス設定のタスク リスト, （57 ページ）

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 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。

関連トピック

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, （106 ページ）

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。

IM アドレス スキームとデフォルトのドメイン

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* は、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。

（注） 選択した IM アドレス スキームは、すべての IM and Presence Service クラスタ全体で一致している必要があります。

UserID@Default_Domain の IM アドレス スキームを使用している場合、IM アドレスの一部として使用されているデフォルトのドメインは、クラスタ全体の設定になります。

UserID@Default_Domain を使用した IM アドレス

UserID@Default_Domain の IM アドレス スキームは、IM and Presence Service を新規インストールまたは以前のバージョンからアップグレードする場合の、デフォルトのオプションです。デフォルトのドメインを設定するには、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）]>[プレゼンス（Presence）]>[設定（Settings）]>[詳細設定（Advanced Configuration）] を選択します。

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。

Cisco Unified CM の IM and Presence の管理 GUI を使用してディレクトリ URI を設定するには、次の 2 つの方法があります。

- LDAP ディレクトリ ソースからディレクトリ URI を同期します。

  Cisco Unified Communications Manager で LDAP ディレクトリ ソースを追加する場合、ディレクトリ URI の値を設定できます。その後で、ディレクトリ ソースからユーザ データを同期するときに、Cisco Unified Communications Manager はディレクトリ URI を追加します。

（注） Cisco Unified Communications Manager で LDAP ディレクトリとの同期が有効な場合は、電子メール アドレス（mailid）または Microsoft OCS/Lync SIP URI（msRTCSIP-PrimaryUserAddress）にディレクトリ URI をマップできます。

- Cisco Unified Communications Manager でディレクトリ URI の値を手動で指定します。

  Cisco Unified Communications Manager で LDAP ディレクトリ ソースを追加しない場合、ディレクトリ URI を自由形式の URI として手動で入力できます。

注意 ディレクトリ URI を IM アドレス スキームとして使用するようにノードを設定する場合、シスコはディレクトリ 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 の IM アドレス スキームが有効な場合、ディレクトリ URI をサポートしていないクライアントは動作しません。ディレクトリ URI をサポートしていないクライアントを展開している場合、シスコは、ディレクトリ URI の IM アドレス スキームではなく、*UserID@Default_Domain* の IM アドレス スキームを使用することを推奨します。

LDAP ディレクトリでディレクトリ URI を設定する場合の詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

IM アドレスの例

次の表は、IM and Presence サービスで使用可能な IM アドレス オプションの例を示しています。

IM and Presence Service Default Domain: cisco.com **User**: John Smith **Userid**: js12345 **Mailid**: jsmith@cisco-sales.com **SIPURI**: john.smith@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（IM Address）**
<userid>@<domain>	適用対象外	js12345@cisco.com
Directory URI	mailid	jsmith@cisco-sales.com
Directory URI	msRTCSIP-PrimaryUserAddress	john.smith@webex.com

Cisco Unified Communications Manager との IM アドレスの統合

Cisco Unified Communications Manager を使用した UserID@Default_Domain の統合

デフォルト IM アドレス スキームは *UserID @ Default_Domain* です。次の条件を満たすすべてのクラスタに対してこの IM アドレス スキームを使用します。

- すべての IM and Presence サービス クラスタが Release 10.0 よりも前のソフトウェア リリースと一緒に展開されます。
- 展開されたクライアントはすべてディレクトリ URI IM アドレス スキームをサポートしません。

名前が示すように、すべての IM アドレスが単一デフォルト IM ドメインの一部です。すべての IM and Presence サービス クラスタ全体で一貫したドメインを設定するために Cisco Unified CM IM and Presence 管理 GUI を使用します。

IM and Presence サービスのIM アドレス（JID）は常に *UserID @ Default_Domain* です。*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（Email address）
- 従業員番号
- 電話番号（Telephone number）

ユーザ ID は電子メール アドレスにマッピングできますが、それが IM URI が電子メール アドレスに等しい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。

Cisco Unified Communications Manager を使用したディレクトリ URI の統合

単一 IM ドメインに限定される *UserID@Default_Domain* IM アドレス スキームとは異なり、Directory URI IM アドレス スキームは複数の IM ドメインをサポートします。ディレクトリ URI に指定されたドメインは IM and Presence Service によってホストされているものとして処理されます。ユーザの IM アドレスを使用して、Cisco Unified Communications Manager で設定されているとおりにそれらのユーザのディレクトリ URI に合わせます。

ディレクトリ URI の形式は自由であり、LDAP から同期することもできます。LDAP 同期が無効になっている場合は、ディレクトリ URI を自由形式の URI として設定することができます。LDAP

ディレクトリ同期が有効になっている場合は、次のフィールドにディレクトリ URI をマッピングできます。

- email address（電子メール アドレス）（mailid）
- Microsoft OCS/Lync SIP URI (msRTCSIP-PrimaryUserAddress)

LDAP の有効化については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

複数の IM ドメインの管理

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。Cisco Unified CM IM and Presence の管理 GUI を使用して、管理者がローカルに管理するドメインを手動で追加、更新、削除し、システムがローカルに管理するすべてのドメインを表示します。

Cisco Expressway と連携させる場合は、ドメインに関する制限の詳細について、『Cisco Expressway Administrator Guide (X8.2)』を参照してください。

セキュリティ

証明書を交換することにより、IM and Presence Service と Cisco Unified Communications Manager 、XMPP クライアント、および SIP クライアントの間にセキュアな接続を設定できます。証明書は自己署名するか、認証局（CA）によって生成されます。

詳細については、セキュリティ設定に関するトピックを参照してください。

シングル サインオン

OpenAM SSO 機能では、システム管理者はWindows ドメインの Windows クライアント マシンにログインでき、再度サインインするよう求められることなく、次のIM and Presence サービス アプリケーションを使用できます。

- Cisco Unified CM IM and Presence の管理
- Cisco Unified IM and Presence サービスアビリティ
- Cisco Unified IM and Presence のレポート
- IM and Presence のディザスタ リカバリ システム
- IM and Presence サービス用のCisco Unified Real-Time Monitoring Tool（RTMT）
- Cisco Unified IM and Presence サービス オペレーティング システムの管理
- Cisco Client Profile Agent：このオプションはCommon Access Card（CAC）サインオンを使用する顧客にのみ適用されます。

Release 10.0 以降では、使用できる 2 種類のシングル サインオン（SSO）があります。

- Security Assertion Markup Language（SAML）SSO
- OpenAM SSO

特に SAML SSO として識別されている場合を除き、SSO への参照は OpenAM SSO を表します。SAML SSO の詳細については、『*Cisco Unified Communications Manager Features and Services Guide*』を参照してください。

第 2 章

マルチノードの拡張性と WAN の展開

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 15,000 ユーザを持つクラスタあたり 45,000 ユーザ
- プレゼンス冗長グループでクラスタあたり 15,000ユーザ、および高可用性の展開でクラスタあたり 45,000 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。

拡張性は、展開内のクラスタの数によって異なります。詳細な VM の設定要件および OVA テンプレートの詳細については、次の url で、「*Virtualization for Unified CM IM and Presence*」を参照してください。http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CM_IM_and_Presence

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*：マルチノードの拡張性オプション

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	**新しいプレゼンス冗長グループへの新しいノードの追加**
平衡型非冗長高可用性展開	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高可用性を提供します。	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高可用性を提供しません。平衡型高可用性を実現するには、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。
平衡型冗長高可用性展開	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高可用性を提供します。 （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高可用性を提供しません。平衡型高可用性を実現するには、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	新しいプレゼンス冗長グループへの新しいノードの追加
アクティブ/スタンバイ冗長高可用性展開	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高可用性が提供されます。これは、高可用性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高可用性を提供しません。高可用性を実現するには、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。

クラスタ全体の DNS SRV

DNS 設定では、クラスタ全体の IM and Presence Service アドレスを定義できます。

Cisco Unified Communications Manager の SIP パブリッシュ トランクは、クラスタ全体の IM and Presence Service アドレスを使用して、Cisco Unified Communications Manager からの SIP パブリッシュ メッセージをクラスタのすべてのノードにロードバランシングします。とりわけ、この設定にすると、初期 SIP パブリッシュ メッセージがクラスタのすべてのノードにロード バランシングされるようになります。また、ノードで障害が発生した場合には、Cisco Unified Communications Manager によって SIP パブリッシュ メッセージが残りのノードに転送されるため、高可用性展開を実現できます。

クラスタ全体の DNS 設定は必須の設定ではありません。クラスタ内のすべてのノードに対して初期 SIP パブリッシュ メッセージをロードバランスする方法としてこの設定方法を推奨します。IM and Presence Service は、各デバイスの後続の SIP パブリッシュ メッセージを IM and Presence Service でユーザが配置されているノードに送信します。

IM and Presence Service が複数のドメインをサポートするとしても、単一のクラスタ全体の DNS SRV レコードのみが必要です。Cisco Unified Communications Manager SIP トランクを設定したときに DNS SRV レコードを指定します。DNS SRV レコードの宛先アドレスとして IM and Presence Service 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任意のドメイン値を指定できます。ただし、IM and Presence Service で SRV クラスタ名を呼び出した SIP プロキシ サービス パラメータが、DNS SRV レコードに指定するドメイン値と一致していることを確認します。指定するドメインにユーザを割り当てる必要はありません。

詳細については、IM and Presence Service および DNS SRV レコードを統合するための Cisco Unified Communications Manager の設定に関するトピックを参照してください。

関連トピック

SIP パブリッシュ トランクのクラスタ全体の DNS SRV 名の設定, （99 ページ）

ローカル フェールオーバー

1 つのプレゼンス冗長グループが 1 つの地理的なサイトにあり、2 番目のプレゼンス冗長グループが別の地理的なサイトにある WAN 経由で IM and Presence Service を展開することもできます。プレゼンス冗長グループにはローカル ノード間の高可用性のために単一ノードまたはデュアル ノードを含めることができます。このモデルは、地理的なサイト間のフェールオーバーを提供しません。

プレゼンス冗長グループの障害検出

IM and Presence Service は、プレゼンス冗長グループの障害検出メカニズムをサポートします。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。IM and Presence Service でハートビート接続とハートビート間隔を設定するには、[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）] > [Server Recovery Manager (service)] を選択します。[一般的な Server Recovery Manager パラメータ（General Server Recovery Manager Parameters）]（クラスタ全体）セクションで、次のパラメータを設定します。

- **[ハートビート間隔（Heart Beat Interval）]**：このパラメータは、Server Recovery Manager が同じ冗長グループのピア Server Recovery Manager にハートビート メッセージを送信する間隔を秒単位で指定します。ハートビートは、ネットワークの可用性を判断するために使用されます。デフォルト値は 60 秒です。
- **[接続タイムアウト（Connect Timeout）]**：このパラメータは、Server Recovery Manager がピア Server Recovery Manager への接続要求から応答を受信するために待つ時間を秒単位で指定します。デフォルト値は 30 秒です。

（注） シスコは、これらのパラメータにデフォルト値を設定することを推奨します。

メソッド イベント ルーティング

WAN 経由で IM and Presence Service を展開する場合は、IM and Presence Service に TCP メソッド イベント ルーティングを設定することを推奨します。メソッドイベントルートを設定するには、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プ

レゼンス（Presence）] > [ルーティング（Routing）] > [メソッド/イベント ルーティング（Method/Event Routing）] を選択します。

外部データベースの推奨事項

WAN展開を介してクラスタリングの外部データベース サーバを設定する場合は、外部データベース サーバを、外部データベース サーバを使用する IM and Presence Service ノードに共存させることを推奨します。

外部データベース サーバおよび M and Presence Service の詳細については、『*Database Setup Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

クラスタ内およびクラスタ間展開における WAN 経由のクラスタリング

IM and Presence Service は、クラスタ内およびクラスタ間展開における WAN 経由のクラスタリング展開をサポートします。

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、クライアントの高可用性をサポートし、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 レベルの高可用性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 Solution Reference Network Design (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 経由の高可用性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。この高可用性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。

関連トピック

WAN 経由のクラスタ内展開, （31 ページ）
http://www.cisco.com/go/designzone

クラスタ間展開

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。

関連トピック

WAN の帯域幅要件, （39 ページ）

クラスタ間ピア関係

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可用

性情報を通信およびサブスクライブできます。あるクラスタからクラスタ間ピアを削除した場合は、リモート クラスタの対応するピアも削除する必要があります。

IM and Presence Service は、ホーム クラスタ アソシエーションのユーザ情報の検索に AXL/SOAP インターフェイスを使用します。IM and Presence Service は、このユーザ情報を使用して、ユーザがローカルユーザ（ホームクラスタのユーザ）であるのか、それとも同じドメイン内のリモート IM and Presence Service クラスタのユーザであるのかを検出します。

IM and Presence Service は登録および通知トラフィックに XMPP インターフェイスを使用します。IM and Presence Service が同じドメイン内のリモート クラスタのユーザを検出すると、IM and Presence Service はリモート クラスタにメッセージを再ルーティングします。

注意 最初の同期で大量の帯域幅と CPU が使用されるため、クラスタ間ピアは時間をずらして設定することを推奨します。複数のピアを同時に設定すると、同期の時間が極端に長くなる可能性があります。

クラスタ間ルータ ツールータ接続

デフォルトでは、IM and Presence Service は、クラスタ間ルータツールータ 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。

IM and Presence Service がクラスタ間ルータツールータ コネクタ ノード間の接続を確立するには、ローカル クラスタとリモート クラスタの両方のノードすべてで Cisco XCP Router サービスを再起動する必要があります。一方のクラスタの各クラスタ間ルータツールータ コネクタは、もう一方のクラスタのルータツールータ コネクタとのクラスタ間接続を開始するか、または受け入れます。

（注） クラスタ間展開では、クラスタに新しいノードを追加すると、ローカル クラスタとリモート クラスタの両方のノードすべてで Cisco XCP Router を再起動する必要があります。

関連トピック

セキュアなクラスタ間ルータ ツー ルータ接続, （35 ページ）

クラスタ間展開のノード名の値

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。

（注） ノード名としてのホスト名の指定がサポートされるのは、すべてのクラスタのすべてのノードが同じ DNS ドメインを共有している場合だけです。

注目 Cisco Jabber クライアントを使用している場合、IP アドレスを IM and Presence Service のノード名として設定すると、証明書の警告メッセージが表示されることがあります。Cisco Jabber で証明書の警告メッセージを生成しないようにするには、ノード名として FQDN を使用してください。IM and Presence Service のノード名の値を設定する手順については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

関連トピック

クラスタ間展開の IM and Presence のデフォルト ドメイン値, （34 ページ）

クラスタ間展開の IM and Presence のデフォルト ドメイン値

クラスタ間展開を設定する場合は、次の点に注意してください。

- クラスタ間機能を正常に動作させるには、ローカルクラスタとリモートクラスタの両方で、IM and Presence のデフォルト ドメイン値が一致している必要があります。

詳細な手順については、IM and Presence のデフォルト ドメインの設定に関するトピックを参照してください。

関連トピック

IM and Presence Service のデフォルトのドメイン設定
クラスタ間展開のノード名の値, （33 ページ）

クラスタ間展開の 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。

詳細については、IM アドレス スキームの設定に関するトピックを参照してください。

関連トピック

IM アドレス スキームの設定, （75 ページ）
UserID@Default_Domain を使用した IM アドレス, （21 ページ）
ディレクトリ URI を使用した IM アドレス, （21 ページ）

セキュアなクラスタ間ルータ ツー ルータ接続

クラスタ間とクラスタ間のルータツールータ接続の組み合わせである、IM and Presence サービス展開内のすべてのルータツールータ コネクタ間にセキュアな XMPP 接続を設定できます。[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [設定（Settings）] を選択し、[XMPP ルータツールータ セキュア モードの有効化（Enable XMPP Router-to-Router Secure Mode）] をオンにします。

XMPP ルータツールータ接続のセキュア モードをオンにすると、IM and Presence サービスは XMPP 信頼証明書を使用してセキュアな SSL 接続を適用します。クラスタ間展開では、IM and Presence サービスは、ローカル クラスタ内にある各ルータツールータ コネクタ ノードとリモート クラスタ内にある各ルータ コネクタ ノード間にセキュアな SSL 接続を適用します。

関連トピック

クラスタ間ルータツールータ接続, （33 ページ）

第 3 章

IM and Presence Service の計画の要件

マルチノード ハードウェアの推奨事項

マルチノード機能を設定するときには、次の点を考慮してください。

- シスコは、展開で高可用性をオンにすることを推奨します。
- シスコは、Cisco Unified Computing System サーバまたはシスコ認定サードパーティ サーバ設定のみで、IM and Presence Service の仮想化した展開をサポートしています。シスコは、Cisco Media Convergence Server（MCS）サーバでは、IM and Presence の展開をサポートしません。仮想化環境での IM and Presence Service の展開の詳細については、http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment を参照してください。
- 展開の数を最小限に抑えます。たとえば、仮想マシンを 5 台使用して計 2,000 人のユーザをサポートするのではなく、仮想マシンを 2 台使用して計 5,000 人のユーザをサポートします。
- 同世代のサーバ ハードウェアを使用します。
- 展開のどのノードにも同種のハードウェアを使用します。同種のハードウェアの世代をいくつか混在させる必要がある場合は、古いハードウェアの同世代のものを同じプレゼンス冗長グループにまとめ、このプレゼンス冗長グループのユーザ数を、高性能の世代を配置したプ

レゼンス冗長グループよりも少なくします。ただし、このような展開にすることはお勧めしません。

警告 マルチノード展開の場合、混在仮想マシンの展開サイズを使用するのではなく、同じプレゼンス冗長グループ内の IM and Presence Service サブスクライバ ノードとデータベース パブリッシャ ノードで、データベース サイズを同様にすることを強く推奨します。2 台のノード間でデータベース サイズが大きく異なると、サブスクライバ ノードのインストール中にエラーを受信します。

マルチノード機能に対応したサポート対象のハードウェアのリストおよびマルチノード機能のハードウェア ユーザ割り当てガイドラインについては、次の URL にある IM and Presence Service の互換性マトリクスを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html

クラスタ間のハードウェアの推奨事項

クラスタ間展開を計画するときは、クラスタ間のすべてのユーザ データを同期できるように、企業内のすべての IM and Presence Service クラスタで類似した展開を使用することを推奨します。たとえば、5,000 人のユーザ展開をサポートしている仮想サーバをクラスタ A 内で使用する場合、クラスタ B に必要なユーザ数が 500 人のみの場合でも、5,000 人のユーザ展開の仮想サーバをクラスタ B で使用する必要があります。

サポートされているエンド ポイント

マルチノードのスケーラビリティ機能は、次のエンドポイントをサポートします。

- Cisco Unified Communications Manager（デスクフォン）
- Cisco Jabber
- サードパーティ XMPP クライアント
- Cisco Unified Mobile Communicator
- Microsoft Office Communicator（Microsoft ソフト クライアント）
- Lotus Sametime（Lotus ソフト クライアント）

（注） Lotus クライアントは、リモート コール制御用 IM and Presence Service と連動する Microsoft サーバで使用されます。

- サードパーティ インターフェイス クライアント
- Lync 2010 および 2013 クライアント（Microsoft Office Communicator）

サードパーティのクライアントだけが、ディレクトリ URI IM アドレス スキームをサポートします。他のすべてのクライアントは *USERID @ Default_Domain* IM アドレス スキームを使用する必要があります。詳細については、IM and Presence Service の IM アドレス スキームに関連する項目を参照してください。

サポートされる LDAP ディレクトリ サーバ

IM and Presence Service は次の LDAP ディレクトリ サーバと統合されます。

- Microsoft Active Directory 2000、2003、および 2008
- Netscape Directory Server
- Sun ONE Directory Server 5.2
- OpenLDAP

関連トピック

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html
http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

WAN の帯域幅要件

最低でも、ラウンドトリップ遅延が 80 ミリ秒以内となるように、各 IM and Presence サービスのプレゼンス冗長グループに 5 Mbps の帯域幅を専用にする必要があります。これらの帯域幅の推奨事項は、クラスタ間およびクラスタ間 WAN 展開に適用されます。帯域幅がこの推奨事項未満の場合、パフォーマンスに悪影響を及ぼす場合があります。

（注） WAN 展開経由のクラスタリングに追加する各 IM and Presence サービスのプレゼンス冗長グループは追加（専用）の 5 Mbps の帯域幅が必要です。

WAN の帯域幅の考慮事項

WAN 上のクラスタリング展開に必要な帯域幅を計算する場合は、次の点を考慮します。

- 帯域幅を考慮する場合、Cisco Unified Communications Manager クラスタの通常の帯域幅使用量を含める必要があります。マルチノードを設定した場合、Cisco Unified Communications Manager はラウンドロビン メカニズムを使用して SIP/SIMPLE メッセージをロード バランシングしますが、より多くの帯域幅が消費されます。パフォーマンスを改善し、トラフィックを減らすために、IM and Presence Service と Cisco Unified Communications Manager との間で送信されるすべての SIP/SIMPLE メッセージに対して単一の専用の Cisco Unified Communications Manager ノードをプロビジョニングできます。

- 帯域幅を考慮する場合、Cisco Unified Personal Communicator ユーザの連絡先リストにおける連絡先の数および IM and Presence のユーザプロファイルのサイズを考慮することを推奨します。WAN 経由で IM and Presence を展開する場合の連絡先リストのサイズに関する推奨事項については、IM and Presence SRND を参照してください。IM and Presence Service の連絡先リストの最大サイズが 200 であるため、多数のユーザを含むシステムの帯域幅については、この点を考慮する必要があることにも注意してください。

詳細については、『*IM and Presence Service Solution Reference Network Design*（*SRND*）』を参照してください。

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/uc7_0.html

マルチノードの拡張性とパフォーマンス

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 15,000 ユーザを持つクラスタあたり 45,000 ユーザ
- プレゼンス冗長グループでクラスタあたり 15,000 ユーザ、および高可用性の展開でクラスタあたり 45,000 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。

拡張性は、展開内のクラスタの数によって異なります。詳細な VM の設定要件および OVA テンプレートの詳細については、次の url で、「*Virtualization for Unified CM IM and Presence*」を参照してください。http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CM_IM_and_Presence

マルチノード パフォーマンスの推奨事項

次の場合はマルチノード機能で最適なパフォーマンスを実現できます。

- すべての IM and Presence Service ノードのリソースは、メモリ、ディスク サイズ、および保持時間の観点からは同等です。仮想サーバのハードウェアのクラスが混在していると、ノードの能力が十分に発揮されず、良好なパフォーマンスが得られません。
- 仮想サーバのハードウェア推奨事項に準拠したハードウェアを展開します。
- バランス モードの展開モデルを設定します。この場合、ユーザの総数は、すべてのプレゼンス冗長グループ内のすべてのノードに均等に分散されます。最適なパフォーマンスを実現するために、IM and Presence Service はデフォルトでバランス モードのユーザ割り当てを行います。

関連トピック

マルチノード ハードウェアの推奨事項, （37 ページ）
平衡型ユーザ割り当て冗長高可用性展開

ユーザ ライセンスの要件

IM and Availability 機能にノード ライセンスまたはソフトウェア バージョン ライセンスは必要ありません。ただし、各 IM and Presence サービス ユーザへ IM and Availability 機能を割り当てる必要があります。

各ユーザに関連付けられているクライアントの数に関係なく、ユーザ単位で IM and Availability を割り当てることができます。IM and Availability をユーザに割り当てると、そのユーザは IM の送受信が可能になり、可用性のアップデートも送受信できます。ユーザで IM and Availability が有効になっていない場合、そのユーザは可用性の更新が許可されません。

Cisco Unified Communications Manager の [エンド ユーザの設定（End User Configuration）] ウィンドウでユーザの IM and Presence サービス機能を有効にできます。詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

IM and Availability 機能は、User Connect Licensing（UCL）と Cisco Unified Workspace Licensing（CUWL）の両方に含まれています。詳細については、『*Cisco Unified Communications Manager Enterprise License Manager User Guide*』を参照してください。

DNS ドメインとデフォルト ドメインの要件

次の DNS ドメインと IM and Presence Service のデフォルト ドメインの条件が適用されます。ドメイン関連の展開の問題を解決するため、クラスタ内のすべての IM and Presence Service のノード名をホスト名ではなく、FQDN または IP アドレスに設定することを推奨します。

- クラスタ間 IM and Presence Service の展開の場合、各 IM and Presence Service クラスタは基礎となっている同じ DNS ドメインを共有している必要があります。
- 任意のクライアント デバイスに関連付けられている DNS ドメインは、IM and Presence Service DNS ドメインにマッピングする必要があります。
- DNS ドメインが IM and Presence Service のデフォルト ドメインに合っていることを確認します。

  IM and Presence Service のデフォルト ドメイン値は、インストール中に DNS ドメインにデフォルトで設定されます。インストール時に IM and Presence Service のデフォルト ドメインは変更できません。DNS ドメインとは異なる値にデフォルト ドメインを変更するには、Cisco Unified CM IM and Presence の管理 GUI を使用する必要があります。

⚠

注意 クラスタ内のすべての IM and Presence Service ノード名をホスト名ではなく FQDN または IP アドレスに設定できない場合は、クラスタ内のノード間の通信障害になる可能性があります。関連する機能には、SIP および XMPP ベースのクラスタ間通信、高可用性、クライアント サイン イン、および SIP ベースのリスト サブスクリプションが含まれます。

第 4 章

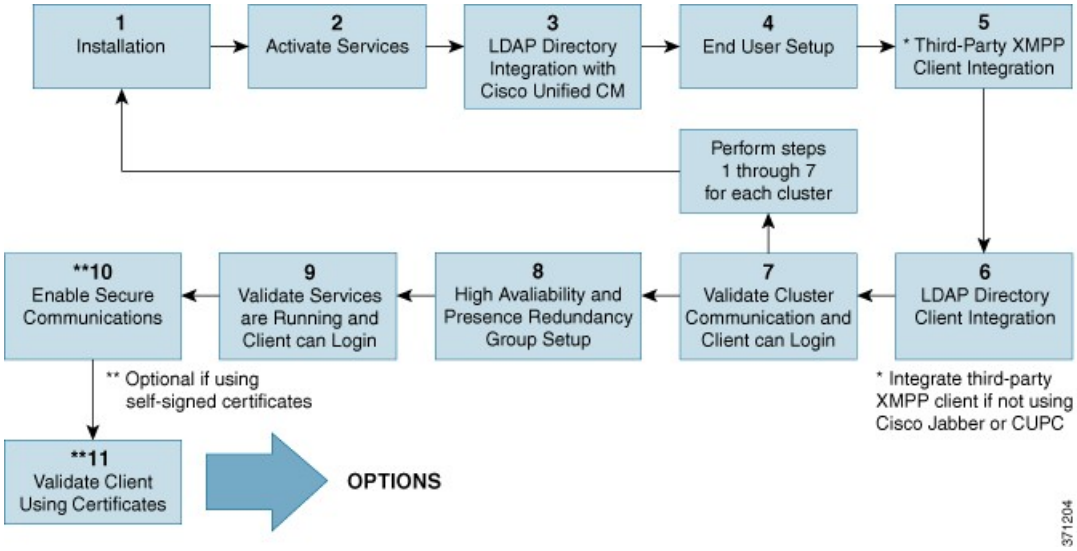
ワークフロー

高可用性の基本的な展開のワークフロー

次のワークフロー図に、高可用性の基本的な IM and Presence Service 展開を設定するためのハイレベルな手順を示します。基本設定後は、ユーザは基本的な IM 機能、プレゼンス、およびアドホック グループ チャットなどの IM および可用性の中心的な機能にアクセスできます。オプション機能は、ユーザ機能を強化するように設定できます。

より高度な展開シナリオとワークフローについては、電話利用状況の設定およびフェデレーションを含むワークフローに関するトピックを参照してください。

図 *3*：高可用性の *IM and Presence Service* の基本的な展開のワークフロー



次の表に、ワークフローの各タスクについて説明します。

ヒント IM and Presence Service ノードをインストールまたは設定する場合は、次のすべての準備タスクを実行します。展開オプションおよび計画要件に関連するトピックのレビュー

表 *4*：高可用性の基本的なワークフローのタスク リスト

	タスク	説明
1	インストール	詳細なインストール手順については、『*Installing Cisco Unified Communications Manager*』を参照してください。
2	サービスのアクティブ化	ノードをインストールした後に手動で機能サービスをアクティブ化する必要があります。詳細な手順については、『*Installing Cisco Unified Communications Manager*』を参照してください。 **ヒント** ネットワーク サービスは、ノードのインストール後に自動的に起動します。

	タスク	説明
3	Cisco Unified Communications Manager との LDAP ディレクトリの統合	IM and Presence Service ノードの LDAP ディレクトリ統合をセットアップします。 • Cisco Unified Communications Manager と LDAP ディレクトリの接続を保護します。 • IM and Presence Service および LDAP サーバ間の接続を保護します。 **ヒント** Cisco Unified Communications Manager および Cisco Jabber と LDAP サーバの統合は推奨設定です。その他の設定については、LDAP 統合に関するトピックを参照してください。
4	エンド ユーザのセットアップ	IM and Presence Service 展開のノードおよびプレゼンス冗長グループにユーザを割り当てます。IM and Presence Service 展開のノードには手動または自動でユーザを割り当てることができます。ユーザを割り当てる手順については『*Cisco Unified Communications Manager Administration Guide*』を参照してください。**User Assignment Mode for Presence Server の [エンタープライズ パラメータ（Enterprise Parameter）]** を使用して、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。 **ヒント** Cisco Unified CM IM and Presence の管理を使用して、ユーザを移行し、連絡先リストをエクスポートおよびインポートします。
5	サードパーティ製 XMPP クライアントの統合	（任意）Cisco Jabber を使用しない場合は、サードパーティ製 XMPP クライアントを統合します。
6	LDAPディレクトリのクライアントの統合	LDAP ディレクトリとのユーザの統合の設定： • ユーザ プロビジョニングのための LDAP 同期の設定 • LDAP サーバ証明書をアップロードします。 • LDAP ユーザ認証を設定します。 **ヒント** Cisco Unified Communications Manager および Cisco Jabber と LDAP サーバの統合は推奨設定です。その他の設定については、LDAP 統合に関するトピックを参照してください。
7	クラスタ通信とクライアントのログインが可能かどうかの検証	クラスタ内で IM と可用性をやりとりできることを確認します。IM が送受信でき、ユーザの可用性の変化が確認できることを確認します。複数のクラスタを設定する場合は、クラスタ全体の基本的な IM と可用性を検証します。

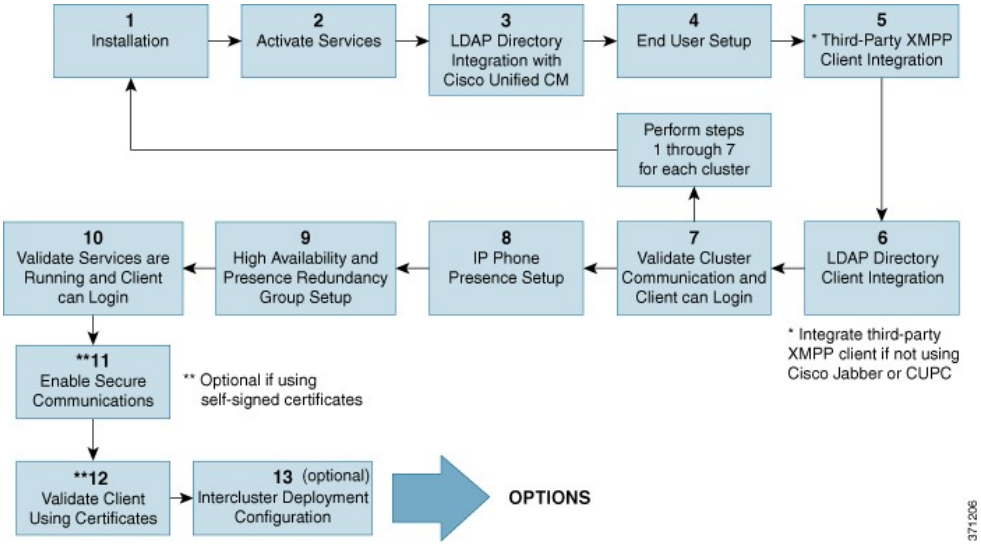
	タスク	説明
8	高可用性とプレゼンス冗長グループの設定	高可用性とプレゼンス冗長性グループを設定する手順については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。
9	サービスが実行されていること、およびクライアントがログインできることの検証	サービスが実行中であることを確認する検証タスクを実行します。クライアントが IM and Presence Service にログインできること、そして可用性があることを確認します。
10	セキュア通信の有効化	IM and Presence Service ノードのセキュア通信を有効化する次のタスクを実行します。 • IM and Presence Service および Cisco Unified Communications Manager 間での証明書の交換を設定します。 • IM and Presence Service に CA 署名付き証明書をアップロードします。 • TLS ピア サブジェクト用に IM and Presence Service の SIP セキュリティを設定します。 •（任意）IM and Presence Service の XMPP セキュリティを設定します。
11	証明書を使用してクライアントを検証します。	クライアントが IM and Presence Service にログインできること、そして可用性があることを確認します。

高可用性と IP Phone プレゼンスを備えた基本展開のワークフロー

次のワークフローの図は、高可用性と IP Phone プレゼンスを備えた、IM and Presence Service の基本展開を設定するハイレベルな手順です。基本設定後に、ユーザは、基本的な IM 機能、プレゼンス、アドホック グループ チャットなど、コア IM と可用性の機能にアクセスできます。オプション機能を設定することで、ユーザ機能を強化することができます。

オプション機能を設定することで、ユーザ機能を強化することもできます。機能オプションやその他の展開ワークフローの詳細については、IM and Presence Service および高可用性展開設定の機能やオプションに関連するトピックを参照してください。

図 *4*：高可用性と *IP Phone* プレゼンスを備えた *IM and Presence Service* の基本ワークフロー



次の表で、ワークフローでの各タスクについて説明します。

表 *5*：高可用性と *IP Phone* プレゼンスを備えた基本ワークフローのタスク リスト

	タスク	説明
1	インストール	詳細なインストール手順については、『*Installing Cisco Unified Communications Manager*』を参照してください。
2	サービスのアクティブ化	ノードをインストールした後に手動で機能サービスをアクティブ化する必要があります。詳細な手順については、『*Installing Cisco Unified Communications Manager*』を参照してください。 **ヒント**　ネットワーク サービスは、ノードのインストール後に自動的に起動します。

	タスク	説明
3	Cisco Unified Communications Manager との LDAP ディレクトリの統合	IM and Presence Service ノードの LDAP ディレクトリ統合をセットアップします。 • Cisco Unified Communications Manager と LDAP ディレクトリの接続を保護します。 • IM and Presence Service および LDAP サーバ間の接続を保護します。 **ヒント** Cisco Unified Communications Manager および Cisco Jabber と LDAP サーバの統合は推奨設定です。その他の設定については、LDAP 統合に関するトピックを参照してください。
4	エンド ユーザのセットアップ	IM and Presence Service 展開のノードおよびプレゼンス冗長グループにユーザを割り当てます。IM and Presence Service 展開のノードには手動または自動でユーザを割り当てることができます。ユーザを割り当てる手順については『*Cisco Unified Communications Manager Administration Guide*』を参照してください。**User Assignment Mode for Presence Server の [エンタープライズ パラメータ（Enterprise Parameter）]** を使用して、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。 **ヒント** ユーザの移行や連絡先リストのエクスポート/インポートを行う場合は、IM and Presence Service の GUI を使用します。
5	サードパーティ製XMPPクライアントの統合	（任意）Cisco Jabber を使用しない場合は、サードパーティ製 XMPP クライアントを統合します。
6	LDAPディレクトリのクライアントの統合	LDAP ディレクトリとのユーザの統合の設定： • ユーザ プロビジョニングのための LDAP 同期の設定 • LDAP サーバ証明書をアップロードします。 • LDAP ユーザ認証を設定します。 **ヒント** Cisco Unified Communications Manager および Cisco Jabber と LDAP サーバの統合は推奨設定です。その他の設定については、LDAP 統合に関するトピックを参照してください。
7	クラスタ通信とクライアントのログインが可能かどうかの検証	クラスタ内で IM と可用性をやりとりできることを確認します。IM が送受信でき、ユーザの可用性の変化が確認できることを確認します。複数のクラスタを設定する場合は、クラスタ全体の基本的な IM と可用性を検証します。

	タスク	説明
8	IP Phone プレゼンスの設定	IM and Presence Service ノードで、次を設定します。 • スタティック ルート • プレゼンス ゲートウェイ • SIP パブリッシュ トランク • SIP パブリッシュ トランクのクラスタ全体での DNS SRV 名
9	高可用性とプレゼンス冗長グループの設定	高可用性とプレゼンス冗長グループを設定する手順については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。
[10]	サービスが実行中であり、クライアントがログイン可能であることの検証	サービスが実行中であることを確認する検証タスクを実行します。クライアントが IM and Presence Service にログインできること、そして可用性があることを確認します。
11	セキュア通信の有効化	次のタスクを実行して、IM and Presence Service ノードでセキュア通信を有効にします。 • IM and Presence Service と Cisco Unified Communications Manager 間で証明書交換を設定します。 • IM and Presence Service に CA 署名付き証明書をアップロードします。 • TLS ピア サブジェクトに対して、IM and Presence Service で SIP セキュリティを設定します。 • （オプション）IM and Presence Service で XMPP セキュリティを設定します。
12	証明書を使用したクライアントの検証	クライアントが IM and Presence Service にログインできること、そして可用性があることを確認します。
13	クラスタ間展開の設定	クラスタ間ピア関係、ルータツールータ接続、ノード名、および IM アドレス スキームを設定します。

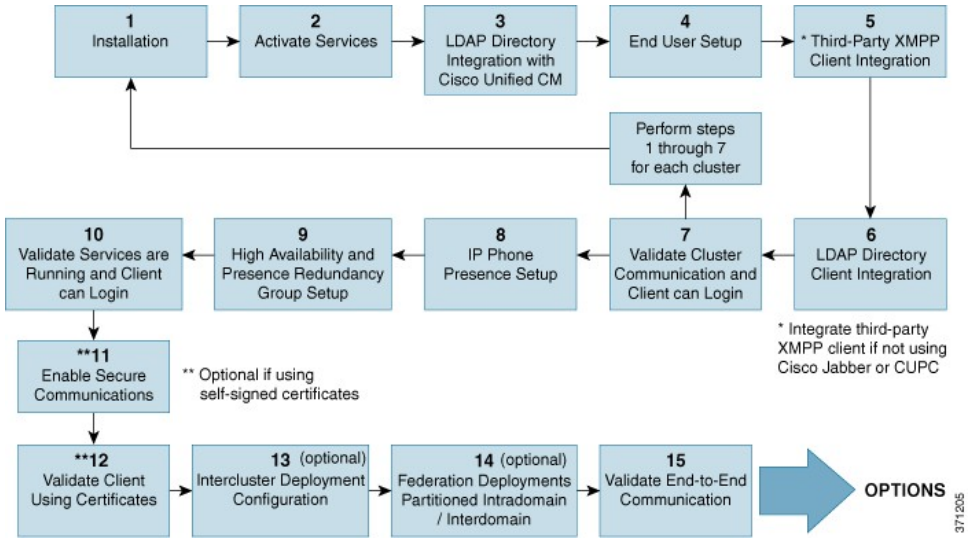
フェデレーション展開のワークフロー

次のワークフローの図は、フェデレーション展開用に、高可用性と IP Phone プレゼンスを備えた、IM and Presence Service の展開を設定する場合の基本的な手順を示しています。フェデレーションの詳細な設定手順については、『*Interdomain Federation for IM and Presence Service on Cisco Unified*

Communications Manager』ガイドおよび『*Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』ガイドを参照してください。

基本設定後に、ユーザは、基本的な IM 機能、プレゼンス、アドホック グループ チャットなど、コア IM と可用性の機能にアクセスできます。オプション機能を設定することで、ユーザ機能を強化することができます。機能オプションの詳細については、IM and Presence Service の機能やオプションに関連するトピックを参照してください。

図 5：***IM and Presence Service*** **のフェデレーション展開用ワークフロー**



次の表で、ワークフローでの各タスクについて説明します。

表 6：***IM and Presence Service*** **のフェデレーション用ワークフローのタスク リスト**

	タスク	説明
1	インストール	詳細なインストール手順については、『*Installing Cisco Unified Communications Manager*』を参照してください。
2	サービスのアクティブ化	ノードをインストールした後に手動で機能サービスをアクティブ化する必要があります。詳細な手順については、『*Installing Cisco Unified Communications Manager*』を参照してください。 **ヒント**　ネットワーク サービスは、ノードのインストール後に自動的に起動します。

	タスク	説明
3	Cisco Unified Communications Manager との LDAP ディレクトリの統合	IM and Presence Service ノードの LDAP ディレクトリ統合をセットアップします。 • Cisco Unified Communications Manager と LDAP ディレクトリの接続を保護します。 • IM and Presence Service および LDAP サーバ間の接続を保護します。 **ヒント** Cisco Unified Communications Manager および Cisco Jabber と LDAP サーバの統合は推奨設定です。その他の設定については、LDAP 統合に関するトピックを参照してください。
4	エンド ユーザのセットアップ	IM and Presence Service 展開のノードおよびプレゼンス冗長グループにユーザを割り当てます。IM and Presence Service 展開のノードには手動または自動でユーザを割り当てることができます。ユーザを割り当てる手順については『*Cisco Unified Communications Manager Administration Guide*』を参照してください。**User Assignment Mode for Presence Server の [エンタープライズ パラメータ（Enterprise Parameter）]** を使用して、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。 **ヒント** ユーザの移行や連絡先リストのエクスポート/インポートを行う場合は、IM and Presence Service の GUI を使用します。
5	サードパーティ製 XMPP クライアントの統合	（オプション）Cisco Jabber または Cisco Unified Communications Manager を使用していない場合は、サードパーティ製 XMPP クライアントを統合します。
6	LDAP ディレクトリのクライアントの統合	LDAP ディレクトリとのユーザの統合の設定： • ユーザ プロビジョニングのための LDAP 同期の設定 • LDAP サーバ証明書をアップロードします。 • LDAP ユーザ認証を設定します。 **ヒント** Cisco Unified Communications Manager および Cisco Jabber と LDAP サーバの統合は推奨設定です。その他の設定については、LDAP 統合に関するトピックを参照してください。
7	クラスタ通信の検証	クラスタ内で IM と可用性をやりとりできることを確認します。IM が送受信でき、ユーザの可用性の変化が確認できることを確認します。複数のクラスタを設定する場合は、クラスタ全体の基本的な IM と可用性を検証します。

	タスク	説明
8	IP Phone プレゼンスの設定	IM and Presence Service ノードで、次を設定します。 • スタティック ルート • プレゼンス ゲートウェイ（Presence Gateway） • SIP パブリッシュ トランク • SIP パブリッシュ トランクのクラスタ全体での DNS SRV 名
9	高可用性とプレゼンス冗長グループの設定	高可用性とプレゼンス冗長グループを設定する手順については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。
10	サービスが実行中であり、クライアントがログイン可能であることの検証	サービスが実行中であることを確認する検証タスクを実行します。クライアントが IM and Presence Service にログインできること、そして可用性があることを確認します。
11	セキュア通信の有効化	次のタスクを実行して、IM and Presence Service ノードでセキュア通信を有効にします。 • IM and Presence Service と Cisco Unified Communications Manager 間で証明書交換を設定します。 • IM and Presence Service に CA 署名付き証明書をアップロードします。 • TLS ピア サブジェクトに対して、IM and Presence Service で SIP セキュリティを設定します。 • （オプション）IM and Presence Service で XMPP セキュリティを設定します。
12	証明書を使用したクライアントの検証	クライアントが IM and Presence Service にログインできること、そして可用性があることを確認します。
13	クラスタ間展開の設定	クラスタ間ピア関係、ルータツールータ接続、ノード名、および IM アドレス スキームを設定します。

	タスク	説明
18	フェデレーション展開	ドメイン間フェデレーションまたはパーティション化されたドメイン内フェデレーションを展開に設定します。手順と要件については、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』および『*Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。
15	エンドツーエンド通信の検証	エンドツーエンド通信を確認する検証タスクを実行します。クラスタ全体で IM と可用性をやりとりできることを確認します。IM が送受信できること、ユーザの可用性でその変更が表示できることを確認します。

IM-Only 展開のワークフロー

ここでは、IM-only IM and Presence Service の展開に必要な設定について説明します。

（注） 強化された IM アドレス指定オプションは、IM-only IM and Presence Service の展開で使用できます。

次の表で、IM-only 展開を設定するタスクについて説明します。

表 7：***IM-Only IM and Presence Service* 展開のタスク リスト**

タスク	説明
Cisco Unified Communications Manager での IM and Presence Service ユーザの作成とライセンス供与	次の URL にある『Cisco Unified Communications Manager』のマニュアルを参照してください。 http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
Cisco Jabber のための LDAP サーバの統合	Cisco Jabber ユーザが LDAP ディレクトリから連絡先を検索できるように、IM and Presence Service で LDAP を設定します。 （注） Cisco Jabber クライアントが IM and Presence Service にある LDAP プロファイルを現在統合していない場合でも、LDAP プロファイルを作成し、LDAP 属性マッピングを検証する必要があります。

ディレクトリ要件と設定の詳細については、Cisco Jabber クライアントの該当するマニュアルを参照してください。

第 II 部

システム設定（System Configuration）

第 5 章

IM and Presence Service と統合するための Cisco Unified Communications Manager の設定

統合前の Cisco Unified Communications Manager のユーザおよびデバイス設定のタスク リスト

IM and Presence Service と統合するように Cisco Unified Communications Manager を設定する前に、次のユーザおよびデバイス設定が Cisco Unified Communications Manager で完了していることを確認します。

表 *8*：*IM and Presence Service* と統合する前に、*Cisco Unified Communications Manager* のユーザとデバイスを設定するためのタスク リスト

タスク	説明
ユーザ クレデンシャル ポリシーを修正する	この手順は、Cisco Unified Communications Manager Release 6.0 以降と統合する場合にだけ適用されます。 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 の管理（Cisco Unified CM Administration）] > [ユーザ管理（User Management）] > [クレデンシャル ポリシーのデフォルト（Credential Policy Default）]
電話機を設定し、各電話機に電話番号（DN）を関連付ける	[CTI からデバイスを制御可能（Allow Control of Device from CTI）] チェックボックスをオンにして、電話がクライアントと相互運用できるようにします。 [Cisco Unified CM の管理（Cisco Unified CM Administration）] > [デバイス（Device）] > [電話（Phone）]
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 の管理（Cisco Unified CM Administration）] > [ユーザ管理（User Management）] > [エンド ユーザ（End User）]
ユーザをラインアピアランスに関連付ける	この手順は、Cisco Unified Communications Manager Release 6.0 以降だけに適用されます。 [Cisco Unified CM の管理（Cisco Unified CM Administration）] > [デバイス（Device）] > [電話（Phone）]
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 の管理（Cisco Unified CM Administration）] > [ユーザ管理（User Management）] > [ユーザ グループ（User Group）]

タスク	説明
（任意）ユーザの directoryURI 値を設定する	IM and Presence Service ノードが Directories URI IM アドレス スキームを使用している場合は、ユーザの directoryURI 値を設定する必要があります。ユーザのディレクトリ URI 値は、Cisco Unified Communications Manager LDAP ディレクトリに同期化するか、または手動で更新できます。 LDAP が有効になっていない場合に LDAP を有効にする、またはユーザのディレクトリ URI 値を手動で編集する手順については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

（注） メニュー オプションおよびパラメータは、Cisco Unified Communications Manager リリースごとに異なる可能性があるため、リリースに適用される Cisco Unified Communications Manager のマニュアルを参照してください。

関連トピック

LDAP ディレクトリ統合, （101 ページ）

プレゼンス グループ間登録パラメータの設定

あるプレゼンスグループのユーザが別のプレゼンスグループのユーザの可用性情報に登録することを許可するには、プレゼンス グループ間登録パラメータを有効にします。

制約事項

プレゼンスグループ間登録パラメータを有効にできるのは、デフォルトの標準プレゼンスグループまたは新しいプレゼンス グループの登録権限が [システム デフォルトの使用（Use System Default）] に設定されている場合のみです。プレゼンス グループを設定するには、[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [システム（System）] > [プレゼンス グループ（Presence Groups）] を選択します。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] > [システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。

ステップ 2 [サーバ（Server）] メニューから [Cisco Unified Communications Manager] ノードを選択します。

ステップ 3 [サービス（Service）] メニューから [Cisco CallManager] を選択します。

ステップ 4 [クラスタ全体のパラメータ（システム - プレゼンス）（Clusterwide Parameters （System - Presence））] セクションでデフォルトのプレゼンス グループ間登録に対して [登録の許可（Allow Subscription）] を選択します。

ステップ 5 [保存（Save）] をクリックします。

ヒント Cisco Unified Communications Manager で IM and Presence Service をアプリケーション サーバとして手動で追加する必要はありません。

次の作業

Cisco Unified Communications Manager の SIP トランクを設定します。

Cisco Unified Communications Manager の SIP トランク設定

SIP トランクに設定するポート番号は、展開する IM and Presence Service のバージョンによって異なります。IM and Presence Service Release 9.0(x) 以降では、SIP トランクにポート番号 5060 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 プロファイルの設定

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] > [システム（System）] > [セキュリティ（Security）] > [SIP トランプ セキュリティ プロファイル（SIP Trunk Security Profile）] を選択します。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 [Non Secure SIP Trunk Profile] をクリックします。

ステップ 4 [コピー（Copy）]をクリックして、[ファイル名（Name）]フィールドにCUPトランクを入力してください。

ステップ 5 [デバイス セキュリティ モード（Device Security Mode）] の設定が [非セキュア（Non Secure）] であることを確認します。

ステップ 6 [着信転送タイプ（Incoming Transport Type）] の設定が [TCP+UDP] であることを確認します。

ステップ 7 [発信転送タイプ（Outgoing Transport Type）] の設定が [TCP] であることを確認します。

ステップ 8 次の項目をオンにして有効にします。

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

ステップ 9 [保存（Save）]をクリックします。

次の作業

Cisco Unified Communications Manager の SIP トランクの設定に進みます。

IM and Presence サービスの SIP トランクの設定

Cisco Unified Communications Manager クラスタと IM and Presence サービス クラスタの間には、1 個の SIP トランクのみを設定します。SIP トランクを設定した後、[Cisco Unified CM の管理（Cisco Unified CM Administration）]> [システム（System）]> [サービス パラメータ（Service Parameters）] を選択することにより、Cisco Unified Communications Manager でその SIP トランクを IM and Presence PUBLISH トランクとして割り当てる必要があります。

[宛先アドレス（Destination Address）] フィールドで、次の形式の 1 つを使用して値を入力してください。

- ドット付き IP アドレス
- 完全修飾ドメイン名（FQDN）

- DNS SRV

高可用性が IM and Presence クラスタに設定されている場合、クラスタ内の複数のノードを識別するために、複数のエントリをドット付き IP アドレスまたは FQDN で入力する必要があります。高可用性を設定する場合は、DNS SRVは IM and Presence のクラスタに使用できません。

はじめる前に

- Cisco Unified Communications Manager の SIP トランク セキュリティ プロファイルを設定します。
- プレゼンス ゲートウェイの設定オプションのトピックを参照してください。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] > [デバイス（Device）] > [トランク（Trunk）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [トランク タイプ（Trunk Type）] メニューから [SIP トランク（SIP Trunk）] を選択します。

ステップ 4 [デバイス プロトコル（Device Protocol）] メニューから [SIP（SIP）] を選択します。

ステップ 5 [トランク サービス タイプ（Trunk Service Type）] で [なし（None）] を選択します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [デバイス名（Device Name）] に「CUPS-SIP-Trunk」と入力します。

ステップ 8 [デバイス プール（Device Pool）] メニューからデバイス プールを選択します。

ステップ 9 ウィンドウの下部にある [SIP 情報（SIP Information）] セクションで、次の値を設定します。

a) [宛先アドレス（Destination Address）] フィールドに、ドット付き IP アドレスまたは DNS で解決可能で、IM and Presence ノードで設定された SRV クラスタ名に一致する必要がある FQDN を入力します。

b) マルチノード展開を設定した場合は、[宛先アドレスはSRVです（Destination Address is an SRV）] をオンにします。
このシナリオでは、Cisco Unified Communications Manager は名前（たとえば、*_sip._tcp.hostname.tld*）を解決するために DNS SRV レコード クエリーを実行します。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し、Cisco Unified Communications Manager は名前（たとえば、*hostname.tld*）を解決するために DNS A レコード クエリーを実行します。

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。

c) [接続先ポート（Destination Port）] に「5060」と入力します。
d) [SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] メニューから [非セキュアな SIP トランク プロファイル（Non Secure SIP Trunk Profile）] を選択します。
e) [SIP プロファイル（SIP Profile）] メニューから [標準 SIP プロファイル（Standard SIP Profile）] を選択します。

ステップ 10 [保存（Save）] をクリックします。

トラブルシューティングのヒント

ポート番号または IP アドレスを変更することで Publish SIP trunk SRV レコードの DNS エントリを修正する場合は、そのアドレスに以前にパブリッシュしたデバイスをすべて再起動し、どのデバイスも正しい IM and Presence サービスの連絡先を指していることを確認する必要があります。

関連トピック

SIP パブリッシュ トランクのクラスタ全体の DNS SRV 名の設定, （99 ページ）
IM and Presence サービスの SIP トランク セキュリティ プロファイルの設定, （61 ページ）
IM and Presence サービスの SIP パブリッシュ トランクの設定, （98 ページ）
プレゼンス ゲートウェイの設定オプション, （97 ページ）

クラスタ外の Unified Communications Manager の電話利用状況の設定

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。クラスタ外にある Cisco Unified Communications Manager からのデフォルトの要求は、IM and Presence Service では受け付けられません。また、Cisco Unified Communications Manager の SIP トランクも設定できます。

TLS ピア サブジェクトを設定する前に、TLS コンテキストを設定する必要があります。

TLS ピア サブジェクトの設定

IM and Presence Service がクラスタ外の Cisco Cisco Unified Communications Manager から SIP PUBLISH を受け入れるようにするには、Cisco 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

ステップ 1 [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）] > [TLS ピア サブジェクト（TLS Peer Subjects）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [ピア サブジェクト名（Peer Subject Name）] フィールドに外部 Cisco Cisco Unified Communications Manager の IP アドレスを入力します。

ステップ 4 [説明（Description）] フィールドにノードの名前を入力します。

ステップ 5 [保存（Save）] をクリックします。

次の作業

TLS コンテキストを設定します。

TLS コンテキストの設定

TLS コンテキストを設定するには、次の手順を使用します。

はじめる前に

TLS ピア サブジェクトを設定します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [TLS コンテキストの設定（TLS Context Configuration）] を選択します。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 [Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context] をクリックします。

ステップ 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。

ステップ 5 この TLS ピア サブジェクトを [Selected TLS Peer Subjects] に移動します。

ステップ 6 [保存（Save）]をクリックします。

ステップ 7 OAMAgent を再起動します。

ステップ 8 Cisco Presence Engine を再起動します。

ヒント 次の順序で再起動し、変更を有効にします。

必要なサービスが Cisco Unified Communications Manager で実行されていることの確認

Cisco Unified Communications Manager サービスは、Cisco Unified Communications Manager ノード、または IM and Presence Service ノードから表示、起動、停止できます。次の手順には、Cisco Unified Communications Manager ノードで従う手順が示されています。Cisco Unified Communications Manager サービスを IM and Presence Service ノードから表示するには、[Cisco Unified IM and Presence の有用性（Cisco Unified IM and Presence Serviceability）] > [ツール（Tools）] > [サービスのアクティブ化（Service Activation）] を選択します。

手順

ステップ 1 Cisco Unified Communications Manager で、[Cisco Unified 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）] を選択します。

ステップ 2 [サーバ（Server）] メニューから [Cisco Unified Communications Manager] ノードを選択します。

ステップ 3 次のサービスが実行されていることを確認します。

- [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）

ヒント Cisco Unified Communications Manager のサービスを有効にするには、[Cisco Unified Serviceability] > [ツール（Tools）] > [サービスのアクティブ化（Service Activation）] を選択します。

第 6 章

IM and Presence Service のネットワーク設定

設定変更通知およびサービス再起動通知

サービス再起動通知

Cisco Unified CM IM and Presence の管理で IM and Presence XCP サービスに影響する設定変更を行う場合は、変更を有効にするために XCP サービスを再起動する必要があります。IM and Presence Service は、設定変更が影響する正確なノードおよび再起動する必要があるサービスを通知します。アクティブな通知のポップアップ ウィンドウが Cisco Unified CM IM and Presence の管理の各ページに表示され、サービスを再起動する必要があることを視覚的に示します。マウスをダイアログバブルアイコンに合わせると、アクティブな通知（存在する場合）および関連する重大度の一覧が表示されます。アクティブな通知のリストから Cisco Unified IM and Presence Serviceability に直接アクセスして、必要なサービスを再起動できます。

特にネットワークに IM and Presence Service を展開した後で設定変更を行う場合は、サービス再起動通知のサービス再起動ポップアップ ウィンドウをモニタすることを推奨します。付属マニュアルのほとんどのタスクでは、サービスの再起動が必要かどうかが示されます。

サービス通知のタイプおよびサービス通知のセキュリティ レベルに関する情報については、サービス再起動通知のオンライン ヘルプ トピックを参照してください。

Cisco XCP Router の再起動

すべての可用性およびメッセージング サービスが IM and Presence Service で適切に機能するには、Cisco XCP Router を実行する必要があります。これは、SIP ベースと XMPP ベースの両方のクライアント メッセージングに適用されます。Cisco XCP ルータを再起動すると、IM and Presence Service によりすべてのアクティブな XCP サービスが自動的に再起動されます。

このモジュールのトピックは、設定変更後に Cisco XCP Router を再起動する必要があるかどうかを示します。Cisco XCP ルータは、停止して再開するのではなく、再起動する必要があります。Cisco XCP Router を再起動するのではなく停止した場合、IM and Presence Service により他のすべての XCP サービスが停止されます。その後 XCP ルータを起動しても、IM and Presence Service により他の XCP サービスは自動的に起動されません。手動で他の XCP サービスを起動する必要があります。

Cisco XCP ルータ サービスの再起動

手順

ステップ 1 IM and Presence サービスで、[Cisco Unified IM and Presence のサービサビリティ（Cisco Unified IM and Presence Serviceability）] > [ツール（Tools）] > [コントロール センター - ネットワーク サービス（Control Center - Network Services）] を選択します。

ステップ 2 ノードを [サーバ（Server）] リストボックスから選択して、[進む（Go）] を選択します。

ステップ 3 [IM and Presence サービス（IM and Presence Service）] セクションで、[Cisco XCP ルータ（Cisco XCP Router）] サービスの横にあるオプション ボタンをクリックします。

ステップ 4 [再起動（Restart）] をクリックします。

ステップ 5 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。

DNS ドメイン コンフィギュレーション

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。いくつかのサンプル ノード展開オプションは、次のとおりです。

（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 ドメインに展開できます。

詳細情報については、『*Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service*』を参照してください。

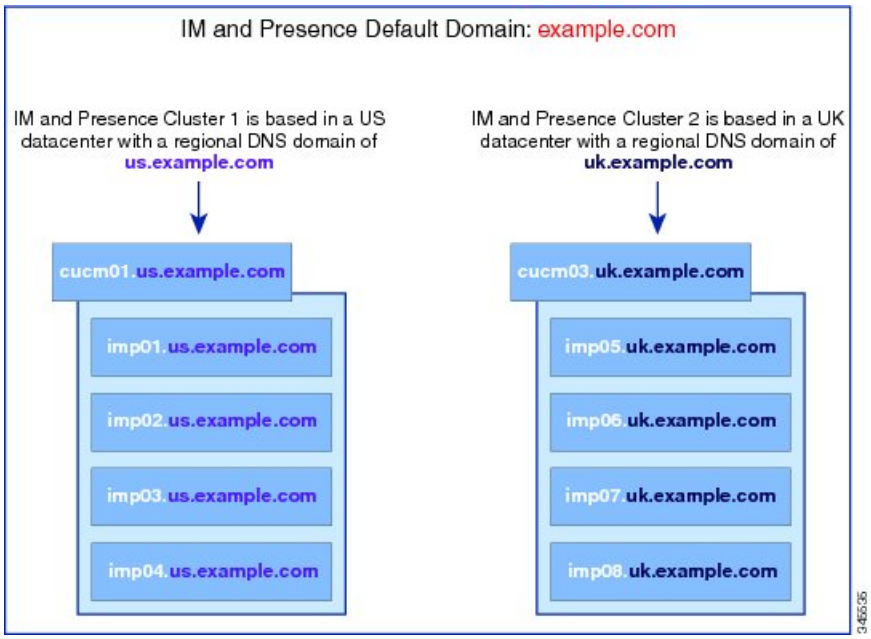
関連トピック

Cisco Unified Communications Manager クラスタに関連付ける DNS ドメインの指定, （72 ページ）
IM and Presence Service のデフォルトのドメイン設定
ノード名の推奨事項

別々の 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

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。

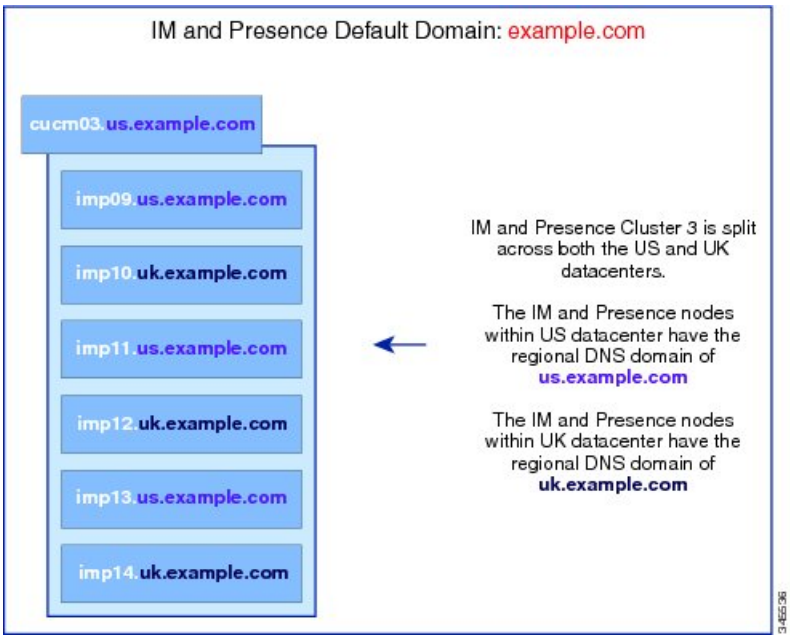
図 *6*：別々の *DNS* ドメインまたはサブドメインに展開された *IM and Presence Service* クラスタ



別々の DNS ドメインまたはサブドメインに展開されたクラスタ内の IM and Presence Service ノード

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。

図 *7*：別々の *DNS* ドメインまたはサブドメインに展開されたクラスタ内の *IM and Presence Service* ノード

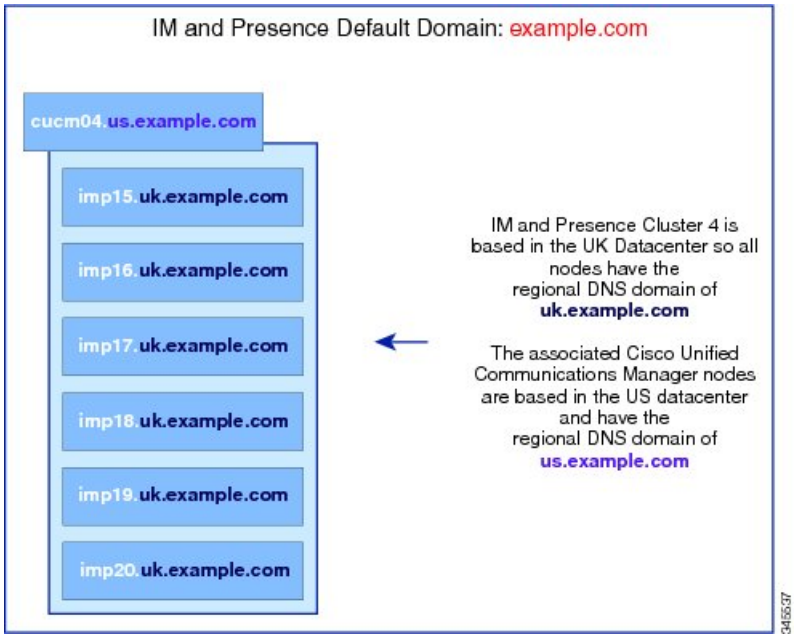


（注） 高可用性は、プレゼンス冗長グループ内の 2 台のノードが別々の DNS ドメインまたはサブドメインにあるシナリオでも完全にサポートされます。

関連する Cisco Unified Communications Manager クラスタとは異なる DNS ドメインに展開されているクラスタ内の IM and Presence Service ノード

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。

図 *8*：関連する *Cisco Unified Communications Manager* クラスタとは異なる *DNS* ドメインに展開されているクラスタ内の *IM and Presence Service* ノード



（注） Cisco Unified Communications Manager との可用性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、CUCM ドメインの SIP Proxy 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ます。したがって、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、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 の管理 GUI を使用してこのサービス パラメータを更新する必要があります。詳細については、トピック「*Specify DNS domain associated with Cisco Unified Communications Manager*」を参照してください。

Cisco Unified Communications Manager クラスタに関連付ける DNS ドメインの指定

（注） この手順は、IM and Presence データベース パブリッシャ ノードの DNS ドメインが Cisco Unified Communications Manager ノードの DNS ドメインとは異なる場合にのみ必要です。

IM and Presence サービスはクラスタ内のすべての Cisco Unified Communications Manager ノード用の アクセス コントロール リスト（ACL）エントリを維持します。これにより、ノード間での可用性のシームレス共有が可能になります。これらの ACL エントリは FQDN ベースであり、Cisco Unified Communications Manager のホスト名を IM and Presence データベース パブリッシャ ノードの DNS ドメインに付加することによって生成されます。

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 ノードの DNS ドメインとは異なる場合、無効な ACL エントリが追加されます。これを回避するには、IM and Presence データベース パブリッシャ ノードの Cisco Unified CM IM and Presence の管理 GUI で次の手順を実行する必要があります。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。

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

ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco SIP プロキシ（Cisco SIP Proxy）] を選択します。

ステップ 4 Cisco Unified Communications Manager ノードの DNS ドメインと一致するように [一般的なプロキシ パラメータ（クラスタ全体）（General Proxy Parameters（Clusterwide））] セクションの [CUCM ドメイン（CUCM Domain）] フィールドを編集します。
デフォルトで、このパラメータは 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ます。

ステップ 5 [保存（Save）]をクリックします。

関連トピック

DNS ドメイン コンフィギュレーション, （68 ページ）

IM and Presence Service のデフォルトのドメイン設定

クラスタ内で IM and Presence Service のデフォルト ドメイン 値を変更する場合、この手順に従ってください。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。

注意 この手順の一環として、サービスを停止する前に、プレゼンス冗長グループの高可用性を無効にします。高可用性が有効な間にサービスを停止すると、システムのフェールオーバーが行われます。

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 Service 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、『*Changing IP Address and Hostname for Cisco Unified Communications Manager and IM and Presence Service*』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。

手順

ステップ 1 表示された順番で、クラスタ内のすべての IM and Presence Service ノードで次のサービスを停止します。

- Cisco Client Profile Agent
- Cisco XCP Router
  （注） Cisco XCP ルータを停止すると、すべての XCP 機能サービスは自動的に停止します。
- Cisco Sync Agent
- Cisco SIP Proxy
- Cisco Presence Engine

ステップ 2 IM and Presence Service データベース パブリッシャ ノードで、新しいドメイン値を設定するには、次のステップを実行します。

a) [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] > [詳細設定（Advanced Configuration）] を選択します。

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

c) [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。

ステップ 3 クラスタ内のすべてのノードで、手動でこの手順の初めで停止したすべてのサービスを起動します。
クラスタ内のすべてのノードで、前に実行されていた、XCP機能サービスを手動で再起動します。

IM アドレス設定

IM アドレスの設定要件

M 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。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。

次のサービスは、IM アドレス スキームを設定する前に、クラスタ内のすべてのノードで停止させる必要があります。

- Cisco Client Profile Agent
- Cisco XCP Router
- Cisco Sync Agent
- Cisco SIP Proxy
- Cisco Presence Engine

IM and Presence Service で IM アドレスを設定する前に、各 IM アドレスに固有の詳細な要件については連動操作と制約事項についてのトピックを、追加情報については IM アドレス設定の計画のトピックを参照してください。

UserID @ Default_Domain IM アドレス インタラクションと制約事項

次の制約事項は *USERID @ Default_Domain* IM アドレス スキームに適用します。

- すべての 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。
- IM アドレス スキームは、すべての IM and Presence Service クラスタ全体で一貫している必要があります。
- 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。
- *UserID* が Cisco Unified Communications Manager の LDAP フィールドにマップされる場合、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。

ディレクトリ URI IM アドレスの連携動作と制約事項

複数のドメイン設定をサポートするには、IM and Presence Service の IM アドレス スキームとしてディレクトリ URI を設定する必要があります。

注意 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 スキームを使用する場合は、次の制約事項および連係動作を順守します。

- すべてのユーザに Cisco Unified Communications Manager に有効なディレクトリ URI 値が設定されています。
- 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 ベースのディレクトリ統合を使用する必要があります。
- UDS ベースのディレクトリ統合はサポートされています。Jabber については、Jabber のリリース 10.6 以降を実行している必要があります。
- すべての IM and Presence Service クラスタで IM アドレス スキームが一貫している必要があります。
- すべてのクラスタが、ディレクトリ URI アドレス スキームをサポートする Cisco Unified Communications Manager のバージョンを実行している必要があります。
- LDAP 同期が無効になっている場合は、ディレクトリ URI を自由形式の URI として設定することができます。LDAP ディレクトリ同期が有効になっている場合は、ディレクトリ URI を電子メール アドレス（mailid）または Microsoft OCS/Lync SIP URI（msRTCSIP-PrimaryUserAddress）にマップできます。
- 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。

IM アドレス スキームの設定

新規インストールする、または以前のバージョンから IM and Presence Service をアップグレードするとき、*UserID @ Default_Domain* IM アドレス スキームがデフォルトのオプションです。Cisco Unified CM IM and Presence Administration GUI を使用して IM and Presence Service クラスタの IM address スキームを設定できます。

注意 この手順の一環として、サービスを停止する前に、プレゼンス冗長グループの高可用性を無効にします。高可用性が有効な間にサービスを停止すると、システムのフェールオーバーが行われます。

（注） 選択した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。

はじめる前に

- クラスタのすべての IM and Presence Service ノードで次のサービスを停止します。
  - Cisco Client Profile Agent
  - Cisco XCP Router

    （注） Cisco XCP ルータを停止すると、すべての XCP 機能サービスは自動的に停止します。
  - Cisco Sync Agent
  - Cisco SIP Proxy
  - Cisco Presence Engine
- クラスタに現存するすべての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。

（注） エンドユーザが正しくプロビジョニングされているか、また、無効または重複ユーザがないかを判断するために、IM and Presence Service トラブルシュータを使用します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] > [詳細設定（Advanced Configuration）] を選択します。**[詳細設定（Advanced Configuration）]** ウィンドウが表示されます。

ステップ 2 [IM アドレス スキーム（IM Address Scheme）] を選択し、[ユーザ ID @ [デフォルト ドメイン]（UserID @ [Default Domain]）] または [ディレクトリ URI（Directory URI）] を選択します。

ヒント IM and Presence Service の要求サービスを停止した後でのみ、IM アドレス スキームが使用可能になります。

ステップ 3 [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）] 設定が無効に設定されている場合は、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。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。

次の作業

システムが正常に更新された場合、クラスタの停止しているすべてのサービスと前に実行されている XCP 機能サービスを再起動できます。設定を確認するには、トラブルシュータを使用します。

IM アドレス タスク フローの設定

システムの IM アドレスを設定するには、次のタスクを完了します。

（注） 既存の IM ユーザ アドレスを編集するだけで、デフォルト ドメインまたは IM アドレス スキームを変更しない場合は、手順 4 に進むことができます。

手順

	コマンドまたはアクション	目的
ステップ 1	サービスの停止, （78 ページ）	IM アドレスの設定を更新する前に、基本の IM and Presence Service を停止する必要があります。
ステップ 2	IM アドレス スキームの割り当て, （79 ページ）	デフォルト ドメイン、IM アドレス スキームなどの新しい設定によって IM アドレスの設定を更新します。
ステップ 3	サービスの再起動, （80 ページ）	基本の IM and Presence Service を再起動します。ユーザ アドレスを更新したりユーザをプロビジョニングしたりする前に、サービスを再起動する必要があります。
ステップ 4	IM ユーザ アドレスの更新	Cisco Unified Communications Manager で対応するユーザ設定を設定することにより、IM ユーザ アドレスを更新します。設定した IM アドレス スキームによって、どのエンドユーザ情報が IM アドレスを取得するかが決まります。

	コマンドまたはアクション	目的
		詳細については、次の場所にある『*Cisco Unified Communications Manager Administration Guide*』の「End User Setup」の章を参照してください： http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

サービスの停止

IM アドレス スキームの設定を更新する前に、基本の IM and Presence Service を停止します。必ず所定の順序でサービスを停止してください。

はじめる前に

サービスを停止する前に高可用性を無効にします（設定している場合）。そのようにしないと、システム フェールオーバーが発生します。

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『*System Configuration Guide for Cisco Unified Communications Manager*』の「Presence Redundancy Groups」の章を参照してください。

手順

ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] から、[ツール（Tools）] > [コントロール センター - ネットワーク サービス（Control Center – Network Services）] を選択します。

ステップ 2 次の IM and Presence Service を停止します。この順序で、サービスを選択し、[停止（Stop）] ボタンをクリックしてください。

a) Cisco Sync Agent
b) Cisco Client Profile Agent

ステップ 3 両方のサービスが停止したら、[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、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

ステップ 4 両方のサービスが停止したら、[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、次のサービスを停止します。

- Cisco XCP Router

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

次の作業

サービスが停止したら、IM アドレス スキームを更新できます。

IM アドレス スキームの割り当て, （79 ページ）

IM アドレス スキームの割り当て

新しいドメインおよび IM アドレス スキームを設定したり、既存のドメインおよびアドレス スキームを更新したりするには、次の手順を使用します。

（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。

はじめる前に

アドレス スキームを設定する前にサービスを停止する必要があります。詳細については、次を参照してください。

サービスの停止, （78 ページ）

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] で、[プレゼンス（Presence）] > [設定（Settings）] > [詳細設定（Advanced Configuration）] を選択します。

ステップ 2 新しいデフォルト ドメインを割り当てるには、[デフォルト ドメイン（Default Domain）] チェック ボックスにマークを付け、テキスト ボックスに新しいドメインを入力します。

ステップ 3 アドレス スキームを変更するには、[IM Address Scheme（IM アドレス スキーム）] チェック ボックスにマークを入れ、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 ドメインとともに取得されます。これがデフォルトの設定です。
- [ディレクトリ URI（Directory 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。

ステップ 4 [保存（Save）] をクリックします。
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）] 設定が無効に設定されている場合は、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。

次の作業

アドレス スキームが割り当てられると、サービスを再起動できます。

サービスの再起動, （80 ページ）

サービスの再起動

IM アドレス スキームを設定したら、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。必ず所定の順序でサービスを起動してください。

はじめる前に

IM アドレス スキームの割り当て, （79 ページ）

手順

ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] から、[ツール（Tools）] > [コントロール センター - ネットワーク サービス（Control Center – Network Services）] を選択します。

ステップ 2 サービスを選択し、[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

ステップ 3 サービスが起動したら、[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、次のサービスをこの順序で起動します。

a) Cisco SIP Proxy
b) Cisco Presence Engine

ステップ 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中であることを確認します。

ステップ 5 [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、次のサービスをこの順序で起動します。

a) Cisco Client Profile Agent
b) Cisco Sync Agent

次の作業

サービスが起動したら、エンドユーザ IM アドレスを更新できます。IM アドレスは、設定されている IM アドレス スキームに応じて Cisco Unified Communications Manager でプロビジョニングされるユーザ ID またはディレクトリ URI から取得されます。

詳細については、次の場所にある『*Cisco Unified Communications Manager Administration Guide*』の「End User Setup」の章を参照してください： http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

IM and Presence Service クラスタのドメイン管理

Cisco Unified CM IM and Presence の管理 GUI を使用して、ローカル IM アドレス ドメインを手動で追加、更新、削除できます。

[IM and Presence ドメイン（IM and Presence Domain）] ウィンドウに次のドメインが表示されます。

- 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。有効化または無効化するドメインはありません。

Cisco Sync 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、そのドメインは管理者が管理するドメインからシステムが管理する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、ドメインは管理者が管理するドメインに戻ります。

（注） 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おり、ディレクトリ URI IM アドレッシングが設定されていることを確認します。

IM ドメイン管理のインタラクションと制約事項

- ローカルクラスタに関連付けられている管理者が管理するドメインのみを追加または削除できます。
- システムが管理するドメインは編集できません。

- 他のクラスタに関連付けられている、システムが管理するかまたは管理者が管理するドメインは編集できません。
- 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。
- 一部のセキュリティ証明書は、手動でドメインを追加、更新、または削除した後で再作成することが必要になる場合があります。自己署名証明書または証明書署名要求（CSR）を生成すると、サブジェクト共通名（CN）がノードの FQDN に設定されます。また、ローカルの IM and Presence のデフォルト ドメインおよび システムがホストするすべての追加ドメインが、サブジェクトの別名（SAN）として証明書に追加されます。
- TLS による XMPP フェデレーションでは、IM アドレス ドメインを追加または削除する場合、TLS 証明書を再作成する必要があります。

IM アドレス ドメインの表示

IM and Presence サービスの展開全体で、システムおよび管理者によって管理されるすべてのプレゼンス ドメインは、[プレゼンス（Presence）] > [ドメイン（Domains）] > [ドメインの検索/一覧表示（Find and List Domains）] ウィンドウに表示されます。いずれかの情報フィールドのチェックマークは、ドメインがローカル クラスタに、または任意のピアのクラスタに関連付けられてるかどうかを示します。管理者が管理するプレゼンス ドメインに関して、次の情報フィールドが表示されます。

- ドメイン
- ローカル クラスタに設定されている
- ピアのクラスタに設定されている

システムが管理するプレゼンス ドメインに関して、次の情報フィールドが表示されます。

- ドメイン
- ローカル クラスタで使用中
- ピアのクラスタで使用中

手順

[Cisco Unified CM IM and Presence Administration] > [プレゼンス（Presence）] > [ドメイン（Domains）] を選択します。**[ドメインの検索と一覧表示（Find and List Domains）]** ウィンドウが表示されます。

IM アドレス ドメインの追加または更新

Cisco Unified CM IM Presence 管理 GUI を使用して、ローカル クラスタに手動で IM アドレス ドメインを追加し、ローカル クラスタにある既存の IM アドレスのドメインを更新できます。

最大255文字のドメイン名を入力でき、各ドメインはクラスタ全体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。

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。IM アドレス ドメインを持つシステムでユーザが設定されていない場合（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。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] > [プレゼンス（Presence）] > [ドメイン（Domains）] 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。

ステップ 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。

ステップ 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。

ヒント 警告メッセージが表示されます。TLS XMPP フェデレーションを使用した場合、新しい TLS 証明書を生成する手順に進みます。

IM アドレス ドメインの削除

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。

システム管理ドメインは使用中の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。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] > [プレゼンス（Presence）] > [ドメイン（Domains）] 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。

ステップ 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。

ステップ 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。

IM and Presence Service のルーティング情報の設定

ルーティング通信の推奨事項

MDNS は IM and Presence Service の XCP ルート ファブリックを確立するためのデフォルトのメカニズムで、ネットワークは、クラスタ内にあるすべての IM and Presence Service ノード間のルータ間接続を自動的に確立します。MDNS ルーティングの要件は、クラスタのすべてのノードが同じマルチキャスト ドメインにあることです。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 ルーティングを推奨します。

ルーティング通信として MDNS を選択する場合は、ネットワークでマルチキャスト DNS を有効にする必要があります。一部のネットワークでは、マルチキャストはデフォルトで有効であるか、特定のネットワーク領域（クラスタを構成するノードが含まれている領域など）で有効です。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 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。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。

または、展開にルータ間通信を選択できます。この場合、IM and Presence Service は動的にクラスタ内のノード間のすべてのルータ間接続を設定します。クラスタのすべてのノードが同じマルチキャスト ドメインにない場合は、このルーティング設定タイプを選択します。ルータ間通信を選択する場合は、次のことに注意してください。

- 展開では、IM and Presence Service が XCP ルート ファブリックを確立している間、追加のパフォーマンスのオーバーヘッドが発生します。
- 新しいノードを追加するときは、展開内のすべてのノードで Cisco XCP Router を再起動する必要はありません。
- ノードを削除する場合は、展開内のすべてのノードで Cisco XCP Router を再起動する必要があります。

MDNS ルーティングとクラスタ ID の設定

インストール時に、システムは固有のクラスタ ID を IM and Presence データベース パブリッシャ ノードに割り当てます。システムはクラスタ ID を配布して、クラスタ内のすべてのノードが同じクラスタ ID 値を共有できるようにします。クラスタ内のノードは、クラスタ ID を使用して、MDNS を使用するマルチキャスト ドメインにある他のノードを識別します。MDNS ルーティングの要件は、1 つのスタンドアロンの IM and Presence サービス クラスタにあるノードが別のスタンドアロン クラスタ内のノードとのルータ間接続を確立することを防ぐために、クラスタ ID 値が一意であることです。スタンドアロン クラスタはクラスタ間ピア接続上でのみ通信します。

クラスタのクラスタ ID 値を表示または設定するには、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）] を選択します。クラスタ ID 値を変更する場合は、値が IM and Presence サービス展開に固有であることを確認します。

（注） チャット機能を導入する場合は、IM and Presence サービスがチャット ノードのエイリアスを定義するクラスタ ID を使用します。クラスタ ID 値の変更が必要になる可能性がある特定の設定シナリオがあります。詳細については、グループ チャット モジュールを参照してください。

関連トピック

チャットの設定と管理, （201 ページ）

ルーティング通信の設定

クラスタ内のノードがメッセージを相互にルーティングできるようにするには、ルーティング通信タイプを設定する必要があります。この設定により、クラスタ内のノード間のルータ接続を確立するためのメカニズムが決定されます。IM and Presence データベース パブリッシャ ノードで

ルーティングの通信タイプを設定し、IM and Presence Service はクラスタのすべてのノードにこのルーティング設定を適用します。

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。

はじめる前に

- MDNS ルーティングを使用する場合は、MDNS がネットワーク内で有効になっていることを確認します。
- ルータ間通信を使用する必要があり、DNS がネットワークで使用できない場合は、ノードごとにクラスタ トポロジでノード名として IP アドレスを設定する必要あります。ノード名を編集するには、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [プレゼンス トポロジ（Presence Topology）] を選択し、ノードの [編集（edit）] リンクをクリックします。この設定は、IM and Presence Service のインストール後、すべてのノードで Cisco XCP Router を再起動する前に実行します。

注目 Cisco Jabber クライアントを使用する時、証明書の警告メッセージは、IP アドレスが IM and Presence Service ノード名として設定されると発生する場合があります。Cisco Jabber で証明書の警告メッセージの生成を防止するには、ノード名として FQDN を使用する必要があります。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。

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

ステップ 3 [サービス（Service）] ドロップダウン リストから [Cisco XCP ルータ（Cisco XCP Router）] を選択します。

ステップ 4 メニューから次の [ルーティング通信タイプ（Routing Communication Types）] のいずれかを選択します。

- [マルチキャスト DNS（MDNS）（Multicast 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。マルチキャスト DNS 通信は、IM and Presence Service でデフォルトで有効になっています。
- [ルータツールータ（Router-to-Router）]：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、ルータツールータ通信を選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 展開内のすべてのノードで Cisco XCP Router サービスを再起動します。

関連トピック

Cisco XCP ルータ サービスの再起動, （68 ページ）

クラスタ ID の設定

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 データベース パブリッシャ ノードに割り当てます。クラスタ内の複数のノードを設定する場合、システムはクラスタの各ノードが同じクラスタ ID 値を共有するようにクラスタ ID を配布します。

クラスタ ID 値をデフォルト設定のままにすることを推奨します。クラスタ ID 値を変更する場合は、次の点に注意してください。

- MDNS ルーティングを選択した場合は、すべてのノードにマルチキャスト ドメインにある他のノードを識別できるようにするために同じクラスタ ID が必要です。
- グループ チャット機能を展開する場合、IM and Presence サービスは、チャット ノードのエイリアス マッピングにクラスタ ID 値を使用し、クラスタ ID 値の変更が必要になる可能性がある特定の設定シナリオがあります。詳細については、グループ チャット モジュールを参照してください。

デフォルトのクラスタ ID 値を変更する場合は、IM and Presence データベース パブリッシャ ノードでのみこの変更を行う必要があります。システムはクラスタ内の他のノードに新しいクラスタ ID 値を複製します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）] を選択します。

ステップ 2 クラスタ ID 値を表示または編集します。

（注） デフォルトでは、IM and Presence サービスはクラスタにクラスタ ID 値の「StandaloneCluster」を割り当てます。

ステップ 3 [保存（Save）] をクリックします。

ヒント 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。

関連トピック

チャットの設定と管理, （201 ページ）

可用性状態変更メッセージのスロットル レートの設定

IM and Presence サービスの過負荷を防ぐために、メッセージで Cisco XCP Router に送信される可用性（プレゼンス）変更のレート（秒当たり）を設定できます。この値を設定すると、IM and Presence サービスは可用性（プレゼンス）変更のレートを設定値に合わせて小さくします。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。

ステップ 2 [サーバ（Server）] 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。

ステップ 3 [サービス（Service）] メニューから [Cisco Presence エンジン（Cisco Presence Engine）] を選択します。

ステップ 4 [クラスタ全体のパラメータ（Clusterwide Parameters）] セクションで、[プレゼンス変更スロットル レート（Presence Change Throttle Rate）] パラメータを編集します。このパラメータは、秒当たりのプレゼンス更新の数を定義します。

ステップ 5 [保存（Save）] をクリックします。

プロキシ サーバの設定

手順

ステップ 1 [Cisco Unified CM IM and Presence 管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [ルーティング（Routing）] > [設定（Settings）] を選択します。

ステップ 2 [メソッド/イベント ルーティングのステータス（Method/Event Routing Status）] で [オン（On）] を選択します。

ステップ 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。

ステップ 4 [保存（Save）] をクリックします。

IM and Presence Service のサービス

IM and Presence サービスのサービスのオン

次の手順は、基本的な IM and Presence サービス設定を導入するときにオンにする必要のあるサービスを一覧表示します。IM and Presence サービス クラスタの各ノードで次のサービスをオンにします。

IM and Presence サービスで導入する追加機能によって他の任意サービスをオンにする必要があります。詳細については、固有の機能に関連する IM and Presence サービス のマニュアルを参照してください。特定のシステム コンポーネントまたは機能を設定できるようにサービスを手動で停止した場合は、この手順を使用して、手動でこれらのサービスを再起動します。

Cisco XCP Router サービスを、基本的な IM and Presence サービス 展開のために実行する必要があります。IM and Presence サービスは、デフォルトで Cisco XCP Router をオンにします。[Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [コントロール センター - ネットワーク サービス（Control Center - Network Services）] を選択して、このネットワーク サービスがオンになっていることを確認します。

手順

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

ステップ 2 [サーバ（Server）] 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。
このメニューから [Cisco Unified Communications マネージャー（Cisco Unified Communications Manager）] ノードを選択して、Cisco Unified Communications Manager サービスのステータスを変更することもできます。

ステップ 3 基本的な IM and Presence サービス展開では、次のサービスをオンにします。

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

ステップ 4 [保存（Save）] をクリックします。

第 7 章

IP Phone Presence の設定

IM and Presence Service のスタティック ルート設定

SIP プロキシ サーバ トラフィック用のスタティック ルートを設定する場合は、次の点を考慮してください。

- ダイナミック ルートは、ルーティング プロトコルとルーティング更新メッセージに従って自動的に計算されるネットワーク経由のパスを表します。
- スタティック ルートは、明示的に設定するネットワーク経由の固定パスを表します。
- スタティック ルートは、ダイナミック ルートよりも優先されます。

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ときは、「.」 に続く文字がスタティック ルートの実際のテレフォニーの数字と一致する必要があります。次のルート組み込みテンプレートのサンプルでは、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 *9*：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	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 *10*：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	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 のルート組み込みテンプレートの設定

最大 5 つのルート組み込みテンプレートを定義できます。ただし、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。

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。

手順

ステップ 1 [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）] を選択します。

ステップ 2 IM and Presence サービス ノードを選択します。

ステップ 3 Cisco SIP Proxy サービスを選択します。

ステップ 4 [（ルーティング パラメータ（クラスタ全体））Routing Parameters（Clusterwide）] セクションの [ルート組み込みテンプレート（RouteEmbedTemplate）] フィールドでルート埋め込みテンプレートを定義します。最大 5 つのルート組み込みテンプレートを定義できます。

ステップ 5 [保存（Save）] を選択します。

次の作業

IM and Presence サービスのスタティック ルートの設定に進みます。

IM and Presence Service のスタティック ルートの設定

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 *11*：*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
[Next Hop（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 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（Route Type）]	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、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（User）] 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（Domain）] 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（Protocol Type）]	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。
[プライオリティ（Priority）]	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
[重み付け（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。
[サービス中（In Service）]	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。 このパラメータを使用すると、管理者は効率的にルートをアウト オブ サービスにすることができます（完全に削除してから再度追加する必要がありません）。
[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。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [ルーティング（Routing）] > [スタティック ルート（Static Routes）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 スタティック ルートを設定します。

ステップ 4 [保存（Save）] をクリックします。

IM and Presence Service のプレゼンス ゲートウェイの設定

プレゼンス ゲートウェイの設定オプション

Cisco Unified Communications Manager と IM and Presence Service との間で可用性情報交換を処理する SIP 接続を有効にするには、IM and Presence Service で Cisco Unified Communications Manager をプレゼンス ゲートウェイとして設定する必要があります。

プレゼンス ゲートウェイを設定するときは、関連する Cisco Unified Communications Manager ノードの FQDN（完全修飾ドメイン名）または IP アドレスを指定します。この値は、使用中のネットワークに応じて次のいずれかになります。

- Cisco Unified Communications Manager データベース パブリッシャ ノードの FQDN アドレス
- Cisco Unified Communications Manager サブスクライバ ノードに解決される DNS SRV FQDN
- Cisco Unified Communications Manager データベース パブリッシャ ノードの IP アドレス

DNS SRV がネットワークのオプション場合は、次の設定を行います。

1. Cisco Unified Communications Manager サブスクライバ ノード（重み付けは均等）の DNS SRV FQDN で IM and Presence Service ノードのプレゼンス ゲートウェイを設定します。これにより、IM and Presence Service では、可用性情報交換に使用するすべてのノード間で可用性 メッセージを均等に共有できます。
2. Cisco Unified Communications Manager で、IM and Presence Service ノードの SIP トランクを IM and Presence Service データベース パブリッシャ ノードとサブスクライバ ノードの DNS SRV FQDN で設定します。

DNS SRV がネットワークのオプションではなく、関連付けられた Cisco Unified Communications Manager ノードの IP アドレスを使用している場合、IP アドレスが単一のサブスクライバ ノードを指すため、複数のサブスクライバ ノードでプレゼンス メッセージング トラフィックを均等に共有できません。

関連トピック

Cisco Unified Communications Manager の SIP トランク設定, （60 ページ）

プレゼンス ゲートウェイの設定

はじめる前に

- プレゼンス ゲートウェイの設定オプションのトピックを参照してください。
- 設定要件に応じて、関連する Cisco Unified Communications Manager ノードの FQDN、DNS SRV FQDN、または IP アドレスを取得します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレセンス（Presence）] > [ゲートウェイ（Gateways）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 [プレゼンス ゲートウェイ タイプ（Presence Gateway Type）] で [CUCM] を選択します。

ステップ 4 [説明（Description）] フィールドにプレゼンス ゲートウェイの説明を入力します。

ステップ 5 [プレゼンス ゲートウェイ（Presence Gateway）] フィールドに、関連付けるCisco Cisco Unified Communications Manager ノードの FQDN、DNS SRV FQDN、または IP アドレスを指定します。

ステップ 6 [保存（Save）] をクリックします。

次の作業

IM and Presence サービスの許可ポリシーを設定します。

関連トピック

IM and Presence サービスの許可ポリシーの設定, （227 ページ）
プレゼンス ゲートウェイの設定オプション, （97 ページ）

IM and Presence サービスの SIP パブリッシュ トランクの設定

この設定をオンにすると、Cisco Cisco Unified Communications Manager は、Cisco Unified Communications Manager で IM and Presence サービス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。

この手順は、Cisco Cisco Unified Communications Manager のサービス パラメータで SIP トランクを CUP PUBLISH トランクとして割り当てる操作と同じです。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）] を選択します。

ステップ 2 [CUCM SIP パブリッシュ トランク（CUCM SIP Publish Trunk）] ドロップダウン リストから [SIP トランク（SIP Trunk）] を選択します。

ステップ 3 [保存（Save）] をクリックします。

SIP パブリッシュ トランクのクラスタ全体の DNS SRV 名の設定

IM and Presence データベース パブリッシャ ノードのクラスタ全体の IM and Presence サービス アドレスを設定すると、IM and Presence サービスはクラスタのすべてのノードのアドレスを複製します。

クラスタ全体の IM and Presence サービスのアドレスを設定すると、SRV ポート値を 5060 に設定します。

（注） IM and Presence サービスのデフォルト ドメインがクラスタ全体の DNS SRV レコードで使用される場合、この手順で SRV クラスタ名の値を変更しないでください。これ以上の操作は必要ありません。

はじめる前に

クラスタ全体の DNS SRV トピックを参照してください。

手順

ステップ 1 [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）] を選択します。

ステップ 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。

ステップ 3 [サービス（Service）] メニューから [Cisco SIP プロキシ（Cisco SIP Proxy）] を選択します。

ステップ 4 [一般的なプロキシ パラメータ（クラスタ全体）（General Proxy Parameters（Clusterwide））] セクションの [SRV クラスタ名（SRV Cluster Name）] フィールドを編集します。
このパラメータはデフォルトでは空です。

ステップ 5 [保存（Save）]をクリックします。

関連トピック

クラスタ全体の DNS SRV, （29 ページ）
展開の拡張性オプション, （28 ページ）

第 8 章

LDAP ディレクトリ統合

LDAP サーバ名、アドレス、およびプロファイル設定

IM and Presence Service の LDAP サーバ名、アドレス、およびプロファイル設定は、Cisco Unified Communications Manager に移動されました。詳細については、『*Cisco Unified Communications Manager Administration Guide, Release 9.0(1)*』を参照してください。

Cisco Unified Communications Manager との LDAP ディレクトリの統合のタスク リスト

次のワークフロー図に、Cisco Unified Communications Manager と LDAP ディレクトリを統合するためのハイレベルな手順を示します。

図 *9*：*Cisco Unified Communications Manager* との *LDAP* ディレクトリの統合のワークフロー

次の表に、タスクを Cisco Unified Communications Manager との LDAP ディレクトリの統合を実行するためのタスクを示します。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 *12* : *LDAP* ディレクトリを統合するためのタスク リスト

タスク	説明
セキュアな Cisco Unified Communications Manager と LDAP ディレクトリとの接続	Cisco Unified Communications Manager の LDAP サーバで Secure Socket Layer（SSL）接続をイネーブルにします。 ヒント　Cisco Unified Communications Manager Release 8.x 以降では、LDAP の SSL 証明書を tomcat-trust 証明書としてアップロードする必要があります。
ユーザ プロビジョニングのための LDAP 同期の設定	Cisco Unified Communications Manager で Cisco Directory Synchronization（DirSync）ツールを有効にし、社内ディレクトリからユーザを自動的にプロビジョニングするか、ユーザ ディレクトリ情報を手動で同期することができます。 ヒント　LDAP 同期は Cisco Unified Communications Manager のアプリケーション ユーザに適用されません。Cisco Unified CM Administration の GUI を使用して、アプリケーション ユーザを手動でプロビジョニングします。
LDAP サーバ証明書のアップロード	Cisco Unified Communications Manager LDAP 認証がセキュア モード（ポート 363 または 3269）に対して設定されている場合、すべての LDAP 認証サーバ証明書と中間証明書を “tomcat-trust” として IM and Presence Service ノードにアップロードする必要があります。
LDAP サーバ認証の設定	Cisco Unified Communications Manager を有効にして、ユーザ パスワードを社内 LDAP ディレクトに対して認証します。 ヒント　LDAP 認証は、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。
IM and Presence Service と LDAP ディレクトリ間のセキュア接続の設定	Cisco Unified Communications Manager と LDAP ディレクトリ間にセキュアな接続を設定した場合は、クラスタのすべての IM and Presence Service ノード上でこのタスクを実行します。

Cisco Unified Communications Manager と LDAP ディレクトリとの間のセキュア接続

Cisco Unified Communications Manager ノードと LDAP ディレクトリ サーバとの間の接続をセキュリティで保護するには、Cisco Unified Communications Manager で LDAP サーバの Secure Socket Layer（SSL）接続を有効にし、SSL 証明書を Cisco Unified Communications Manager にアップロードします。Cisco Unified Communications Manager Release 8.x 以降では、LDAP の SSL 証明書を tomcat-trust 証明書としてアップロードする必要があります。

LDAP の SSL 証明書をアップロードしたら、Cisco Unified Communications Manager で次のサービスを再起動する必要があります。

- ディレクトリ サービス

- Tomcat サービス

Cisco Unified Communications Manager への証明書のアップロードの詳細については、Cisco Unified Communications Manager のマニュアルを参照してください。

ユーザ プロビジョニングのための LDAP 同期の設定

LDAP 同期は Cisco Unified Communications Manager で Cisco Directory Synchronization（DirSync）ツールを使用して、社内 LDAP ディレクトリから情報を（手動または定期的に）同期します。DirSync サービスを有効にすると、Cisco Unified Communications Manager が自動的に社内ディレクトリからのユーザをプロビジョニングします。Cisco Unified Communications Manager は引き続きローカルデータベースを使用しますが、そのファシリティを無効にしてユーザアカウントの作成を可能にします。LDAP ディレクトリ インターフェイスを使用して、ユーザ アカウントを作成および管理します。

はじめる前に

- Cisco Unified Communications Manager で LDAP 固有の設定を試行する前に、LDAP サーバがインストールされていることを確認してください。
- Cisco Unified Communications Manager で Cisco DirSync サービスをアクティブにします。

制約事項

LDAP 同期は Cisco Unified Communications Manager のアプリケーション ユーザに適用されません。Cisco Unified CM の管理インターフェイスでアプリケーション ユーザを手動でプロビジョニングする必要があります。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] > [システム（System）] > [LDAP（LDAP）] > [LDAP システム（LDAP System）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 LDAP サーバのタイプおよび属性を設定します。

ステップ 4 [LDAP サーバからの同期を有効にする（Enable Synchronizing from LDAP Server）] を選択します。

ステップ 5 [Cisco Unified CM の管理（Cisco Unified CM Administration）] > [システム（System）] > [LDAP（LDAP）] > [LDAP ディレクトリ（LDAP Directory）] を選択します。

ステップ 6 次の項目を設定します。

a) LDAP ディレクトリ アカウント設定
b) 同期対象のユーザ属性
c) 同期スケジュール
d) LDAP サーバ ホスト名または IP アドレスおよびポート番号

ステップ 7 Secure Socket Layer（SSL）を使用して LDAP ディレクトリと通信するには、[SSL を使用（Use SSL）] をオンにします。

ヒント
- LDAP over SSL を設定するには、LDAP ディレクトリ証明書を Cisco Unified Communications Manager にアップロードします。
- 特定の LDAP 製品のアカウント同期メカニズムおよび LDAP 同期の一般的なベスト プラクティスの詳細については、Cisco Unified Communications Manager SRND の LDAP ディレクトリの情報を参照してください。

次の作業

LDAP 認証サーバ証明書のアップロードに進みます。

関連トピック

http://www.cisco.com/go/designzone

LDAP 認証サーバ証明書のアップロード

Cisco Unified Communications Manager LDAP 認証をセキュア モード（ポート 636 または 3269）に設定する場合は、認証局（CA）のルート証明書や他のすべての中間証明書などのLDAP認証サーバ証明書を、「tomcat-trust」 として個別に IM and Presence Service ノードにアップロードする必要があります。

手順

ステップ 1 [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）] を選択します。

ステップ 2 [証明書のアップロード（Upload Certificate）] をクリックします。

ステップ 3 [証明書名（Certificate Name）] メニューから [tomcat-trust] を選択します。

ステップ 4 ローカル コンピュータから LDAP サーバ ルート証明書を参照し、選択します。

ステップ 5 [ファイルのアップロード（Upload File）] をクリックします。

ステップ 6 他のすべての中間証明書に対して上記の手順を繰り返します。

次の作業

LDAP 認証の設定に進みます。

LDAP 認証の設定

LDAP 認証機能を使用すると、社内 LDAP ディレクトリに対して Cisco Unified Communications Manager でユーザ パスワードを認証できます。

はじめる前に

Cisco Unified Communications Manager で LDAP 同期を有効にします。

制約事項

LDAP 認証は、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。Cisco Unified Communications Manager は、内部データベースのアプリケーション ユーザを認証します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] > [システム（System）] > [LDAP（LDAP）] > [LDAP 認証（LDAP Authentication）] を選択します。

ステップ 2 ユーザに対する LDAP 認証を有効にします。

ステップ 3 LDAP 認証設定を指定します。

ステップ 4 LDAP サーバ ホスト名または IP アドレスおよびポート番号を設定します。

（注） Secure Socket Layer（SSL）を使用して LDAP ディレクトリと通信するには、[SSL を使用（Use SSL）] をオンにします。

[SSL を使用（Use SSL）] チェックボックスをオンにした場合、IP アドレスまたはホスト名または LDAP サーバの証明書のサブジェクト CN と一致する FQDN を入力します。LDAP サーバの証明書のサブジェクト CN は、IP アドレス、ホスト名、または FQDN である必要があります。この条件を満たさない場合は、Cisco Unified CM IM and Presence の管理、Cisco Unified IM and Presence Serviceability、Cisco Unified IM and Presence リポーティング、Cisco Jabber ログイン、サードパーティ製 XMPP クライアントおよび Cisco Unified Communications Manager の他のアプリケーション、さらにユーザ認証を実行する LDAPに接続している IM and Presence Service のログインの失敗を招くので、[SSL を使用（Use SSL）] のチェックボックスをオンにしないでください。

ヒント LDAP over SSL を設定するには、LDAP ディレクトリ証明書を Cisco Unified Communications Manager にアップロードします。

次の作業

IM and Presence サービスと LDAP ディレクトリ間のセキュア接続の設定

IM and Presence サービスと LDAP ディレクトリ間のセキュア接続の設定

このトピックは、Cisco Unified Communications Manager と LDAP ディレクトリとの間のセキュア接続を設定する場合にのみ適用されます。

（注） クラスタ内のすべての IM and Presence サービス ノードでこの手順を実行します。

はじめる前に

Cisco Unified Communications Manager で LDAP の SSL を有効にし、LDAP ディレクトリ証明書を Cisco Unified Communications Manager にアップロードします。

手順

ステップ 1 [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）] を選択します。

ステップ 2 [証明書のアップロード（Upload Certificate）] をクリックします。

ステップ 3 [証明書の名前（Certificate Name）] メニューから [tomcat-trust] を選択します。

ステップ 4 ローカル コンピュータから LDAP サーバ証明書を参照し、選択します。

ステップ 5 [ファイルのアップロード（Upload File）] をクリックします。

ステップ 6 コマンド `utils service restart Cisco Tomcat` を使用して、CLI から Tomcat サービスを再起動します。

次の作業

Cisco Jabber と LDAP ディレクトリを統合します。

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

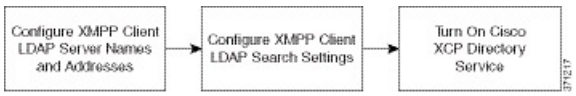
次のトピックでは、サードパーティ製 XMPP クライアントのユーザが LDAP ディレクトリから連絡先を検索および追加できるように IM and Presence Service で LDAP 設定を行う方法について説明します。

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。

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。

図 *10*：*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 *13*：*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 サーバが設定されている場合、LDAP サーバはある時点で 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。

はじめる前に

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。

手順

ステップ 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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 LDAP サーバの ID を入力します。

ステップ 4 LDAPサーバのホスト名を入力します。

ステップ 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。

ステップ 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。

ステップ 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、入力できるホスト名の値は、LDAP サーバのホスト名または FQDN です。使用する値は、セキュリティ証明書の 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、この値が証明書の CN または SAN フィールドにも使用されている必要があります。

ステップ 8 [保存（Save）] をクリックします。

ステップ 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。

次の作業

XMPP クライアントの LDAP 検索の設定に進みます。

関連トピック

Cisco Unified Communications Manager と LDAP ディレクトリとの間のセキュア接続, （102 ページ）
IM and Presence サービスと LDAP ディレクトリ間のセキュア接続の設定, （105 ページ）

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 *14*：*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（ユーザ オブジェクト クラス）	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。
User Attribute（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。

フィールド	設定
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。

はじめる前に

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

ステップ 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。

ステップ 2 次の各フィールドに情報を入力します。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 [保存（Save）] をクリックします。

ステップ 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。

次の作業

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。

はじめる前に

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

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

ステップ 2 [サーバ（Server）] 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。

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

ステップ 4 [保存（Save）] をクリックします。

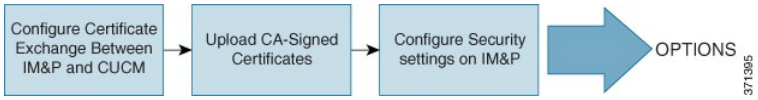
第 9 章

IM and Presence Service のセキュリティ設定

セキュリティ設定のタスク リスト

次のワークフローの図は、IM and Presence サービス ノードの展開のセキュリティを設定するための手順の概要を示します。

図 *11*：セキュリティ設定のワークフロー



次の表は、IM and Presence サービス ノードの展開のセキュリティ設定をするためのタスクを示します。手順の詳細については、ワークフローで説明されているタスクに関連する手順を参照してください。

（注） オプションで、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。

表 *15*：*IM and Presence* サービスのセキュリティ設定のタスク リスト

タスク	説明
IM and Presence サービスと Cisco Unified Communications Manager 間の証明書交換の設定	次の作業を実行します。 • IM and Presence サービス ノードへの Cisco Unified Communications Manager 証明書のインポート後、SIP プロキシ サービスを再起動します。 ヒント [セキュリティ（Security）] > [証明書の管理（Certificate Management）] から [証明書インポート ツール（Certificate Import Tool）] または手動で [Cisco Unified IM and Presence OS の管理（Cisco Unified IM and Presence OS Administration）] を使用して証明書をインポートできます。 • IM and Presence サービスから証明書をダウンロード後、Cisco Unified Communications Manager で証明書を Callmanager-trust にアップロードします。 • Cisco Unified Communications Manager サービスを再起動します。 （注） Cisco Unified Communications Manager と IM and Presence サービス間の証明書交換を設定する前に、IM and Presence サービスのSIP セキュリティ プロファイルと SIP トランクを設定する必要があります。
CA-Signed 証明書のアップロード	単一サーバまたは複数サーバの展開のために、IM and Presence サービスに認証局（CA）署名付き証明書をアップロードします。サービスの再起動が必要です。詳細については、関連タスクを参照してください。 • tomcat 証明書 • cup-xmpp 証明書 • cup-xmpp-s2s 証明書 ヒント クラスタのすべてのIM and Presence サービス ノードで証明書をアップロードできます。証明書のアップロードが完了すると、証明書と関連の署名証明書はクラスタ内の他のすべての IM and Presence サービス ノードに自動的に配布されます。

タスク	説明
IM and Presence サービスでセキュリティ設定をします。	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。 IM and Presence サービスは XMPP ベースの設定でセキュリティが強化されています。[システム（System）] > [セキュリティ（Security）] > [設定（Settings）] から [Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] を使用して IM and Presence サービスの XMPP セキュア モードを設定できます。

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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 4 [参照（Browse）] を選択し .txt ファイルを検索します。

ステップ 5 [ファイルのアップロード（Upload File）] 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 サービス ノードに個別にアップロードする必要があります。

IM and Presence Service の証明書タイプ

ここでは、IM and Presence Service のクライアントとサービスに必要なさまざまな証明書について説明します。

表 *16*：*IM and Presence Service* のクライアント アプリケーションの証明書タイプ

クライアント	証明書
SIP クライアント（Cisco Unified Communications Manager）	tomcat
XMPP クライアント（Cisco Jabber、サードパーティ製クライアント）	cup-xmpp

表 *17*：*IM and Presence Services* の証明書タイプ

サービス	証明書	証明書信頼ストア	注記
SIP Proxy	cup	cup-trust	
Presence Engine	cup	cup-trust	
SOAP	tomcat	directory-trust	
AXL	tomcat	directory-trust	
LDAP	tomcat	directory-trust	LDAP は、directory/directory-trust が tomcat/ttrust であるため、tomcat 証明書を使用します。
Microsoft Exchange		cup-trust	
Microsoft Lync/OCS コール制御	cup	cup-trust	
SIP フェデレーション	cup	cup-trust	
XMPP フェデレーション	Cup-xmpp-s2s	cup-xmpp-trust	cup-xmpp-s2s の信頼証明書は、一般的な XMPP 信頼証明書とともに cup-xmpp-trust に保存されます。

関連トピック

IM and Presence Service の XMPP セキュリティの設定, （136 ページ）
IM and Presence サービスと LDAP ディレクトリ間のセキュア接続の設定, （105 ページ）

IM and Presence Service と Cisco Unified Communications Manager 間の証明書交換の設定

このモジュールでは、Cisco Unified Communications Manager ノードと IM and Presence Service ノード間における自己署名証明書の交換について説明します。IM and Presence Service で証明書インポート ツールを使用して、Cisco Unified Communications Manager 証明書を IM and Presence Service に自動的にインポートできます。ただし、手動で Cisco Unified Communications Manager に IM and Presence Service 証明書をアップロードする必要があります。

IM and Presence Service および Cisco Unified Communications Manager 間にセキュア接続が必要な場合にのみ、次の手順を実行します。

セキュリティを設定するための前提条件

Cisco Unified Communications Manager で次の項目を設定します。

- IM and Presence Service の SIP 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。

関連トピック

Cisco Unified Communications Manager の SIP トランク設定, （60 ページ）

IM and Presence サービスへの Cisco Unified Communications Manager 証明書のインポート

手順

ステップ 1 [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。

ステップ 2 **[証明書信頼ストア（Certificate Trust Store）]** メニューから **[IM and Presence（IM/P）サービス信頼（IM and Presence（IM/P）Service Trust）]** を選択します。

ステップ 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。

ステップ 4 Cisco Unified Communications Manager ノードと通信するポート番号を入力します。

ステップ 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。

次の作業

SIP プロキシ サービスの再起動に進みます。

SIP Proxy サービスの再起動

はじめる前に

IM and Presence サービスに Cisco Unified Communications Manager 証明書をインポートします。

手順

ステップ 1 IM and Presence サービスで [Cisco Unified IM and Presence サービサビリティ（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）] を選択します。

ステップ 2 [Cisco SIP プロキシ（Cisco SIP Proxy）] を選択します。

ステップ 3 [再起動（Restart）] をクリックします。

次の作業

IM and Presence サービスから証明書をダウンロードする手順に進みます。

IM and Presence サービスからの証明書のダウンロード

手順

ステップ 1 IM and Presence サービスで、[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）] を選択します。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 cup.pem ファイルを選択します。

ステップ 4 [ダウンロード（Download）] 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。

次の作業

Cisco Unified Communications Manager に IM and Presence サービス証明書をアップロードします。

Cisco Unified Communications Manager への IM and Presence Service 証明書のアップロード

はじめる前に

IM and Presence Service から証明書をダウンロードします。

手順

ステップ 1 Cisco Unified Communications Manager で [Cisco Unified OS の管理（Cisco Unified OS Administration）] > [セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 2 [証明書のアップロード（Upload Certificate）] をクリックします。

ステップ 3 [証明書名（Certificate Name）] メニューから [Callmanager-trust] を選択します。

ステップ 4 IM and Presence Service から以前にダウンロードした証明書（.pem ファイル）を参照し、選択します。

ステップ 5 [ファイルのアップロード（Upload File）] をクリックします。

次の作業

Cisco Unified Communications Manager CallManager サービスの再起動に進みます。

Cisco Unified Communications Manager サービスの再起動

はじめる前に

Cisco Unified Communications Manager に IM and Presence サービス 証明書をアップロードします。

手順

ステップ 1 Cisco Unified Communications Manager で、[Cisco Unified サービスアビリティ（Cisco Unified 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）] を選択します。

ステップ 2 [Cisco CallManager（Cisco CallManager）] を選択します。

ステップ 3 [再起動（Restart）] をクリックします。

次の作業

IM and Presence サービスの SIP セキュリティ設定に進みます。

関連トピック

IM and Presence Service での SIP セキュリティの設定, （135 ページ）

IM and Presence Service への単一サーバ CA 署名付き証明書のアップロード

ここでは、IM and Presence Service に次のタイプの CA 署名付き証明書をアップロードする方法について説明します。

- tomcat 証明書
- cup-xmpp 証明書
- cup-xmpp-s2s 証明書

CA 署名付きの Tomcat 証明書のタスク リスト

CA 署名付き Tomcat 証明書を IM and Presence Service にアップロードするためのハイレベルな手順は次のとおりです。

1. 署名を行う認証局のルート証明書および中間証明書を IM and Presence Service にアップロードします。

2. Cisco Intercluster Sync Agent サービスを再起動します。
3. CA 証明書が他のクラスタに正しく同期されていることを確認します。
4. 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します。
5. すべてのノードで Cisco Tomcat サービスを再起動します。
6. 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。

署名を行う認証局のルート証明書および中間証明書のアップロード

ルート証明書および中間証明書をアップロードする場合は、証明書チェーンの各証明書をルート証明書から中間証明書の順に IM and Presence Service へアップロードする必要があります。

root > intermediate-1 > intermediate-2 > … > intermediate-N

チェーンでアップロードする各証明書ごとに、以前にアップロードしたどの証明書が署名したかを指定する必要があります。次に、例を示します。

- intermediate-1 の場合は、署名にルート証明書が使用されました。
- intermediate-2 の場合は、署名に intermediate-1 が使用されました。

IM and Presence データベース パブリッシャ ノードで関連のリーフ証明書の信頼ストアにルート証明書および中間証明書（存在する場合）をアップロードする必要があります。署名を行う認証局（CA）のルート証明書および中間証明書を展開された IM and Presence Service にアップロードするには、次の手順を実行します。

手順

ステップ 1 IM and Presence データベース パブリッシャ ノードで、[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）] を選択します。

ステップ 2 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします。

ステップ 3 [証明書名（Certificate Name）] ドロップダウン リストで、[tomcat-trust] を選択します。

ステップ 4 署名付き証明書の説明を入力します。

ステップ 5 [参照（Browse）] をクリックしてルート証明書のファイルを見つけます。

ステップ 6 [ファイルのアップロード（Upload File）] をクリックします。

ステップ 7 **[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）]** ウィンドウを使用して、各中間証明書を同じ方法でアップロードします。

次の作業

Cisco Intercluster Sync Agent サービスを再起動します。

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。このサービスの再起動することにより、ただちに CA 証明書が他のすべてのクラスタに同期されます。

手順

ステップ 1 管理 CLI にログインします。

ステップ 2 次のコマンドを実行します。utils service restart Cisco Intercluster Sync Agent

（注） また、Cisco Unified Serviceability GUI からCisco Intercluster Sync Agent サービスを再起動できます。

次の作業

CA 証明書が他のクラスタに同期したことを確認します。

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。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [診断（Diagnostics）] > [システム トラブルシューター（System Troubleshooter）] を選択します。

ステップ 2 [クラスタ間トラブルシューター（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。

ステップ 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。

ステップ 4 [プレゼンス（Presence）] > [クラスタ間（Inter-Clustering）] を選択し、**[システム トラブルシューター（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。

ステップ 5 [強制手動同期（Force Manual Sync）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

次の作業

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。

各 IM and Presence Service ノードへの署名付き証明書のアップロード

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。

（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。

手順

ステップ 1 [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）] を選択します。

ステップ 2 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします。

ステップ 3 [証明書名（Certificate Name）] ドロップダウン リストで、[tomcat] を選択します。

ステップ 4 署名付き証明書の説明を入力します。

ステップ 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。

ステップ 6 [ファイルのアップロード（Upload File）] をクリックします。

ステップ 7 各 IM and Presence Service ノードで繰り返します。

証明書の管理の詳細については、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

次の作業

Cisco Tomcat サービスを再起動します。

Cisco Tomcat サービスを再起動します。

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

ステップ 1 管理 CLI にログインします。

ステップ 2 次のコマンドを実行します。utils service restart Cisco Tomcat

ステップ 3 各ノードで繰り返します。

次の作業

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

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [診断（Diagnostics）] > [システム トラブルシューター（System Troubleshooter）] を選択します。

ステップ 2 [クラスタ間トラブルシューター（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。

ステップ 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。

ステップ 4 [プレゼンス（Presence）] > [クラスタ間（Inter-Clustering）] を選択し、**[システム トラブルシューター（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。

ステップ 5 [強制手動同期（Force Manual Sync）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 10 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、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。

CA 署名付き cup-xmpp 証明書のアップロード

CA 署名付き cup-xmpp 証明書を IM and Presence Service にアップロードするためのハイレベルな手順は次のとおりです。

1. 署名を行う認証局のルート証明書および中間証明書を IM and Presence Service にアップロードします。
2. Cisco Intercluster Sync Agent サービスを再起動します。

3 CA 証明書が他のクラスタに正しく同期されていることを確認します。
4 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します。
5 すべてのノードで Cisco XCP ルータ サービスを再起動します。

署名を行う認証局のルート証明書および中間証明書のアップロード

ルート証明書および中間証明書をアップロードする場合は、証明書チェーンの各証明書をルート証明書から中間証明書の順に IM and Presence Service へアップロードする必要があります。

root > intermediate-1 > intermediate-2 > … > intermediate-N

チェーンでアップロードする各証明書ごとに、以前にアップロードしたどの証明書が署名したかを指定する必要があります。次に、例を示します。

- intermediate-1 の場合は、署名にルート証明書が使用されました。
- intermediate-2 の場合は、署名に intermediate-1 が使用されました。

IM and Presence データベース パブリッシャ ノードで **cup-xmpp-trust** ストアにルート証明書および中間証明書（存在する場合）をアップロードする必要があります。署名を行う認証局（CA）のルート証明書および中間証明書を展開された IM and Presence Service にアップロードするには、次の手順を実行します。

手順

ステップ 1 IM and Presence データベース パブリッシャ ノードで、[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）] を選択します。

ステップ 2 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします。

ステップ 3 [証明書名（Certificate Name）] ドロップダウン リストから [cup-xmpp-trust] を選択します。

ステップ 4 署名付き証明書の説明を入力します。

ステップ 5 [参照（Browse）] をクリックしてルート証明書のファイルを見つけます。

ステップ 6 [ファイルのアップロード（Upload File）] をクリックします。

ステップ 7 **[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）]** ウィンドウを使用して、各中間証明書を同じ方法でアップロードします。

次の作業

Cisco Intercluster Sync Agent サービスを再起動します。

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。このサービスの再起動することにより、ただちに CA 証明書が他のすべてのクラスタに同期されます。

手順

ステップ 1 管理 CLI にログインします。

ステップ 2 次のコマンドを実行します。utils service restart Cisco Intercluster Sync Agent

（注） また、Cisco Unified Serviceability GUI からCisco Intercluster Sync Agent サービスを再起動できます。

次の作業

CA 証明書が他のクラスタに同期したことを確認します。

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。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [診断（Diagnostics）] > [システム トラブルシューター（System Troubleshooter）] を選択します。

ステップ 2 [クラスタ間トラブルシューター（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。

ステップ 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。

ステップ 4 [プレゼンス（Presence）] > [クラスタ間（Inter-Clustering）] を選択し、**[システム トラブルシューター（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。

ステップ 5 [強制手動同期（Force Manual Sync）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

次の作業

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。

各 IM and Presence Service ノードへの署名付き証明書のアップロード

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 cup-xmpp 証明書をアップロードできます。

（注） クラスタに必要なすべての cup-xmpp 証明書に署名し、それらの証明書を同時にアップロードして、サービスへの影響が単一のメンテナンス時間帯内で管理できるようにすることを推奨します。

手順

ステップ 1 [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）] を選択します。

ステップ 2 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします。

ステップ 3 [証明書名（Certificate Name）] ドロップダウン リストから [cup-xmpp] を選択します。

ステップ 4 署名付き証明書の説明を入力します。

ステップ 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。

ステップ 6 [ファイルのアップロード（Upload File）] をクリックします。

ステップ 7 各 IM and Presence Service ノードで繰り返します。

証明書の管理の詳細については、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

次の作業

すべてのノードで Cisco XCP ルータ サービスを再起動します。

すべてのノードの Cisco XCP Router サービスの再起動

注意 Cisco XCP Router の再起動はサービスに影響を与えます。

各 IM and Presence Service ノードに cup-xmpp 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。

手順

ステップ 1 管理 CLI にログインします。

ステップ 2 次のコマンドを実行します。utils service restart Cisco XCP Router

ステップ 3 各ノードで繰り返します。

（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。

CA 署名付き cup-xmpp-s2s 証明書のアップロード

CA 署名付き cup-xmpp-s2s 証明書を IM and Presence Service にアップロードするためのハイレベルな手順は次のとおりです。

1. 署名を行う認証局のルート証明書および中間証明書を IM and Presence Service にアップロードします。
2. CA 証明書が他のクラスタに正しく同期されていることを確認します。
3. 適切な署名付き証明書を IM and Presence Service フェデレーション ノードにアップロードします（この証明書はフェデレーションに使用する IM and Presence Service ノードにのみ必要であり、すべてのノードに必要なわけではありません）。
4. 影響を受けるすべてのノードで Cisco XCP XMPP Federation Connection Manager サービスを再起動します。

署名を行う認証局のルート証明書および中間証明書のアップロード

ルート証明書および中間証明書をアップロードする場合は、証明書チェーンの各証明書をルート証明書から中間証明書の順に IM and Presence Service へアップロードする必要があります。

root > intermediate-1 > intermediate-2 > … > intermediate-N

チェーンでアップロードする各証明書ごとに、以前にアップロードしたどの証明書が署名したかを指定する必要があります。次に、例を示します。

- intermediate-1 の場合は、署名にルート証明書が使用されました。

- intermediate-2 の場合は、署名に intermediate-1 が使用されました。

IM and Presence データベース パブリッシャ ノードで **cup-xmpp-trust** ストアにルート証明書および中間証明書（存在する場合）をアップロードする必要があります。署名を行う認証局（CA）のルート証明書および中間証明書を展開された IM and Presence Service にアップロードするには、次の手順を実行します。

手順

ステップ 1 IM and Presence データベース パブリッシャ ノードで、[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）] を選択します。

ステップ 2 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします。

ステップ 3 [証明書名（Certificate Name）] ドロップダウン リストから [cup-xmpp-trust] を選択します。

ステップ 4 署名付き証明書の説明を入力します。

ステップ 5 [参照（Browse）] をクリックしてルート証明書のファイルを見つけます。

ステップ 6 [ファイルのアップロード（Upload File）] をクリックします。

ステップ 7 **[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）]** ウィンドウを使用して、各中間証明書を同じ方法でアップロードします。

次の作業

CA 証明書が他のクラスタと同期されたことを確認します。

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。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [診断（Diagnostics）] > [システム トラブルシューター（System Troubleshooter）] を選択します。

ステップ 2 [クラスタ間トラブルシューター（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。

ステップ 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。

ステップ 4 [プレゼンス（Presence）] > [クラスタ間（Inter-Clustering）] を選択し、**[システム トラブルシューター（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。

ステップ 5 [強制手動同期（Force Manual Sync）] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

次の作業

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。

フェデレーション ノードへの署名付き証明書のアップロード

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 フェデレーション 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。すべてのノードに証明書をアップロードする必要はありません。フェデレーション用のノードにだけアップロードします。

（注） クラスタに必要なすべての cup-xmpp-s2s 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。

手順

ステップ 1 [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）] を選択します。

ステップ 2 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします。

ステップ 3 [証明書名（Certificate Name）] ドロップダウン リストから [cup-xmpp] を選択します。

ステップ 4 署名付き証明書の説明を入力します。

ステップ 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。

ステップ 6 [ファイルのアップロード（Upload File）] をクリックします。

ステップ 7 各IM and Presence Service フェデレーション ノードで繰り返します。

証明書の管理の詳細については、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

次の作業

影響を受けるノードで Cisco XCP XMPP Federation Connection Manager サービスを再起動します。

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

ステップ 1 管理 CLI にログインします。

ステップ 2 次のコマンドを実行します。utils service restart Cisco XCP XMPP Federation Connection Manager

ステップ 3 各フェデレーション ノードで繰り返します。

自己署名の信頼証明書の削除

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 Service 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。

IM and Presence Service または Cisco Unified Communications Manager のいずれかで元の自己署名信頼証明書を置き換えるために CA 署名付き証明書が生成されても、元の自己署名信頼証明書は、両方のノードのサービス信頼ストアで保持されます。自己署名信頼証明書を削除する場合には、

IM and Presence Service および Cisco Unified Communications Manager の両方のノードでこれらの証明書を削除する必要があります。

IM and Presence Service からの自己署名信頼証明書の削除

はじめる前に

重要 ここまでで、CA 署名付き証明書で IM and Presence Service ノードを設定し、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 分待機しました。

手順

ステップ 1 **[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 Operating System Administration）]** ユーザ インターフェイスにログインし、[セキュリティ（Security）] > [証明書管理（Certificate Management）]を選択します。

ステップ 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：tomcat-trust
- Cup-xmpp：cup-xmpp-trust
- Cup-xmpp-s2s：cup-xmpp-trust
- Cup：cup-trust
- Ipsec：ipsec-trust

ステップ 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。

ステップ 4 [削除（Delete）] をクリックします。
（注） [削除（Delete）] ボタンは、削除する権限を持っている証明書に関してのみ表示されます。

次の作業

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。

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, （134 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。

はじめる前に

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

ステップ 1 **[Cisco Unifiedオペレーティングシステムの管理（Cisco Unified Operating System Administration）]** ユーザ インターフェイスにログインし、[セキュリティ（Security）] > [証明書管理（Certificate Management）] 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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は、[削除（Delete）] 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。

ステップ 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。

IM and Presence Service での 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

ステップ 1 [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）] > [TLS ピア サブジェクト（TLS Peer Subjects）] の順に選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 ピア 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。

ステップ 4 [説明（Description）] フィールドにノードの名前を入力します。

ステップ 5 [保存（Save）] をクリックします。

次の作業

TLS コンテキストを設定します。

TLS コンテキストの設定

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。

はじめる前に

IM and Presence サービスの TLS ピア サブジェクトを設定します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [TLS コンテキスト設定（TLS Context Configuration）] の順に選択します。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 [Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context] を選択します。

ステップ 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。

ステップ 5 この TLS ピア サブジェクトを [Selected TLS Peer Subjects] に移動します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 [Cisco Unified IM and Presence Serviceability] > [ツール（Tools）] > [サービスの開始（Service Activation）] を選択します。

ステップ 8 Cisco SIP プロキシ サービスを再起動します。

トラブルシューティングのヒント

TLS コンテキストに対する変更を有効にするには、SIP Proxy サービスを再起動する必要があります。

関連トピック

SIP Proxy サービスの再起動, （118 ページ）

IM and Presence Service の XMPP セキュリティの設定

XMPP セキュリティ モード

IM and Presence サービスは XMPP ベースの設定でセキュリティが強化されています。次の表は、これらの XMPP のセキュリティ モードについて説明します。IM and Presence サービスの XMPP セキュリティ モードを設定するには、[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）] > [設定（Settings）] を選択します。

表 *18* : *XMPP* セキュア モードの説明

セキュア モード	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）	この設定をオンにすると、IM and Presence サービスは、クラスタ内の IM and Presence サービス ノードと XMPP クライアント アプリケーション間にセキュアな TLS 接続を確立します。IM and Presence サービスは、このセキュア モードをデフォルトでオンにします。 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。

XMPP のセキュリティ設定を更新した場合は、サービスを再起動します。次のいずれかの操作を行います。

- [XMPP クライアント ツー 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 Mode）] を編集した場合は、Cisco XCP Connection Manager 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。
- [XMPP ルータツールータ セキュア モードの有効化（Enable XMPP Router-to-Router Secure Mode）] を編集した場合は、Cisco XCP Router 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 - ネットワーク サービス（Control Center - Network Services）]を選択して、このサービスを再起動します。
- [Web クライアント ツー IM/P サービスのセキュア モードを有効にする（Enable Web Client to IM/P Service Secure Mode）] を編集した場合は、Cisco XCP Web Connection Manager 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。

関連トピック

IM and Presence サービスと XMPP クライアント間のセキュア接続の設定, （138 ページ）

IM and Presence サービスと XMPP クライアント間のセキュア接続の設定

手順

ステップ 1 [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）] > [設定（Settings）] を選択します。

ステップ 2 次のいずれかの作業を実行します。

- クラスタの IM and Presence サービスと XMPP client アプリケーションの間のセキュアな TLS 接続を確立するには、[Enable XMPP Client To IM/P Service Secure Mode（XMPP クライアント ツー IM/P サービス セキュア モードを有効にする）] を選択します。

  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。

- クラスタの IM and Presence サービスと 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 接続を確立するには、[Web クライアント ツー IM/P サービス セキュア モードを有効にする（Enable Web Client To IM/P Service Secure Mode）] を選択します。

  この設定をオンにする場合は、IM and Presence 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てください。

ステップ 3 [保存（Save）]をクリックします。

XMPP のセキュリティ設定を更新した場合は、次の手順の 1 つを使用して次のサービスを再起動します。

- [XMPP クライアント ツー 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 Mode）] を編集した場合は、Cisco XCP Connection Manager 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。
- [Web クライアント ツー IM/P サービスのセキュア モードを有効にする（Enable Web Client to IM/P Service Secure Mode）] を編集した場合は、Cisco XCP Web Connection Manager 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。

次の作業

IM and Presence サービス ノードの XMPP クライアントをサポートするサービスをオンに設定します。

関連トピック

サードパーティ製クライアントの統合, （19 ページ）

IM and Presence サービスのオンによる XMPP クライアントのサポート

IM and Presence サービス クラスタ内の各ノードでこの手順を実行します。

手順

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

ステップ 2 **[サーバ（Server）]** 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。

ステップ 3 次のサービスをオンにします。

- Cisco XCP Connection Manager：XMPP クライアントまたはIM and Presence サービスの XMPP ベースの API クライアントを統合する場合は、このサービスをオンします。
- Cisco XCP Authentication Service：XMPP クライアント、XMPP ベースの API クライアント、または IM and Presence サービスの XMPP ベースの API クライアントを統合する場合は、このサービスをオンにします。
- Cisco XCP Web Connection Manager：XMPP クライアント、または IM and Presence サービスの XMPP ベースの API クライアントを統合する場合は、このサービスを任意でオンにします。

ステップ 4 [保存（Save）] をクリックします。

ヒント XMPP クライアントが正常に機能するように、クラスタ内のすべてのノードで Cisco XCP Router がオンになっていることを確認します。

関連トピック

サードパーティ製クライアントの統合, （19 ページ）

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* には IM and Presence サービス展開によって設定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 サービス 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」

ヒント　任意のノード上の `cup-xmpp-s2s` 証明書を表示するには、[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、**[cup-xmpp-s2s]** リンクをクリックします。

手順

ステップ 1　[システム（System）] > [セキュリティの設定（Security Settings）] を選択します。

ステップ 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。

ステップ 3　[保存（Save）] をクリックします。

次の作業

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 サービス 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。

第 10 章

クラスタ間ピアの設定

クラスタ間展開の前提条件

スタンドアロンの IM and Presence Service クラスタ内で、IM and Presence データベース パブリッシャ ノード間にクラスタ間ピアを設定します。クラスタ内の IM and Presence Service サブスクライバ ノードには、クラスタ間ピア接続を設定する必要はありません。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。

- クラスタ間ピアをそれぞれ別の Cisco Unified Communications Manager と統合する必要があります。
- ホームの IM and Presence Service クラスタとリモートの IM and Presence Service クラスタの両方で、必要なマルチノード設定を完了する必要があります。
  - 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。
  - クラスタ内の各 IM and Presence Service ノードでサービスをアクティブにします。
- すべてのローカル IM and Presence ノード、およびすべてのリモート IM and Presence ノードで AXL インターフェイスを有効にする必要があります。IM and Presence Service は、デフォルトでは AXL 権限を持つクラスタ間アプリケーション ユーザを作成します。クラスタ間ピアを設定するには、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。
- ローカルの IM and Presence データベース パブリッシャ ノードとリモートの IM and Presence データベース パブリッシャ ノードで Sync Agent をオンにする必要があります。クラスタ間ピアを設定する前に、Sync Agent が Cisco Unified Communications Manager からのユーザの同期化を完了できるようにします。

プレゼンスユーザプロファイルの特定など、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、IM and Presence Service の SRND を参照してください。

クラスタ間ピアの設定

クラスタ間ピアの設定

ローカルの IM and Presence サービス クラスタのデータベース パブリッシャ ノードと（ピア関係を形成するローカル クラスタを有する）リモートの IM and Presence サービス クラスタのデータベース パブリッシャ ノードでこの手順を実行します。

はじめる前に

- すべてのローカル IM and Presence Service ノードで AXL インターフェイスをアクティブにして、すべてのリモート IM and Presence Service ノードで AXL インターフェイスがアクティブであることを確認します。
- Sync Agent がローカル クラスタおよびリモート クラスタの Cisco 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。
- リモートの IM and Presence サービス ノードのクラスタ間アプリケーション ユーザの AXL ユーザ名とパスワードを取得します。
- ネットワークで DNS を使用しない場合は、IM and Presence サービスのデフォルトドメインとクラスタ間展開のノード名の値に関するトピックを参照してください。
- この手順を続行する前に、無効なユーザ ID または重複したユーザ ID を解決します。詳細については、エンド ユーザの管理および処理に関するトピックを参照してください。

（注） クラスタ間ピア接続が正常に機能するには、2 つのクラスタ間にファイアウォールがある場合、次のポートが開いたままになっている必要があります。

- 8443（AXL）
- 7400（XMPP）
- 5060（SIP）（SIP フェデレーション使用時のみ）

制約事項

すべての IM and Presence サービス クラスタのクラスタ間トランク転送として TCP を使用することを推奨します。

手順

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

ステップ 2 リモートの IM and Presence サービス クラスタのデータベース パブリッシャ ノードの IP アドレス、FQDN、またはホスト名を入力します。

ステップ 3 AXL 権限を持つリモートの IM and Presence サービス ノードのアプリケーション ユーザのユーザ名を入力します。

ステップ 4 AXL 権限を持つリモートの IM and Presence サービス ノードのアプリケーション ユーザの関連付けられたパスワードを入力します。

ステップ 5 SIP 通信の優先プロトコルを入力します。

ステップ 6 （任意） 外部電話番号マスク値を入力します。これは、リモート クラスタから取得された電話番号に適用する E.164 マスクです。

ステップ 7 [保存（Save）]をクリックします。

ステップ 8 ローカル クラスタ内のすべてのノードで Cisco XCP Router サービスを再起動します。

ステップ 9 この手順を繰り返してリモートのクラスタ間ピアを作成し、次にリモート 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。

ヒント Sync Agent が（ローカル クラスタまたはリモート クラスタの）Cisco Cisco Unified Communications Manager からのユーザの同期化を完了する前にクラスタ間ピア接続を設定した場合は、クラスタ間ピア接続のステータスは失敗として表示されます。

クラスタ間転送プロトコルとして TLS を選択する場合は、IM and Presence サービスは、クラスタ間ピアの間で証明書を自動的に交換して、セキュアな TLS 接続を確立しようとします。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。

次の作業

続いて Intercluster Sync Agent をオンに設定します。

関連トピック

Cisco XCP ルータ サービスの再起動, （68 ページ）
クラスタ間展開のノード名の値, （33 ページ）
クラスタ間展開の IM and Presence のデフォルト ドメイン値, （34 ページ）
Cisco XCP ルータ サービスの再起動, （68 ページ）
クラスタ間展開のノード名の値, （33 ページ）
クラスタ間展開のデフォルトのドメイン値

Intercluster Sync Agent のオン

デフォルトでは、IM and Presence Service は Intercluster Sync Agent パラメータをオンにします。Intercluster Sync Agent パラメータがオンになっていることを確認するか、または手動でこのサービスをオンにするには、この手順を使用します。

Intercluster Sync Agent は、次の処理のために AXL/SOAP インターフェイスを使用します。

- ユーザが（ローカル クラスタ上の）ローカル ユーザであるか、それとも同じドメイン内のリモート IM and Presence Service クラスタ上のユーザであるかを IM and Presence Service が判断できるように、ユーザ情報を取得します。
- ローカル ユーザへのリモートIM and Presence Service クラスタの変更をクラスタに通知します。

（注） ローカル IM and Presence データベース パブリッシャ ノードからリモート IM and Presence データベース パブリッシャ ノードへのユーザ情報の同期に加えて、Intercluster Sync Agent はクラスタのすべてのノード間のセキュリティも処理するため、IM and Presence Service クラスタ内のすべてのノードで Intercluster Sync Agent をオンにする必要があります。

手順

ステップ 1 [Cisco Unified IM and Presence 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 - ネットワーク サービス（Control Center - Network Services）] を選択します。

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

ステップ 3 [Cisco クラスタ間同期エージェント（Cisco Intercluster Sync Agent）] を選択します。

ステップ 4 [開始（Start）] をクリックします。

次の作業

クラスタ間ピアの状態を確認する手順に進みます。

関連トピック

マルチノードの拡張性機能, （27 ページ）

クラスタ間ピア ステータスの確認

手順

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

ステップ 2 検索条件メニューからピア アドレスを選択します。

ステップ 3 [検索（Find）] をクリックします。

ステップ 4 表示するピア アドレス エントリを選択します。

ステップ 5 **[クラスタ間ピア ステータス（Inter-cluster Peer Status）]** ウィンドウで次の操作を実行します。

a) クラスタ間ピアの各結果エントリの横にチェック マークがあることを確認します。

b) [関連ユーザ（Associated Users）] の値がリモート クラスタのユーザ数と等しいことを確認します。

c) クラスタ間転送プロトコルとして TLS を選択した場合は、[証明書のステータス（Certificate Status）] 項目に TLS 接続のステータスが表示され、IM and Presence Service が正常にクラスタ間でセキュリティ証明書を交換したか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ように）手動で Tomcat 信頼証明書を更新する必要があります。その他の証明書交換エラーについては、オンラインヘルプで推奨処置を確認してください。

ステップ 6 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [診断（Diagnostics）] > [システム トラブルシューター（System Troubleshooter）] を選択します。

ステップ 7 [クラスタ間トラブルシューター（Inter-Clustering Troubleshooter）] セクションで、各クラスタ間ピア接続エントリのステータスの横にチェック マークがあることを確認します。

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

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。具体的には、既存の [クラスタ間ピア設定（Inter-cluster Peer Configuration）] ウィンドウで、新しいリモート クラスタを指すように [ピア アドレス（Peer Address）] 値を変更します。このエラーは、初めて IM and Presence をインストールしたとき、または IM and Presence Service のホスト名またはドメイン名を変更した場合、あるいは Tomcat 証明書を再生成した場合にも発生することがあります。

この手順では、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方法について説明します。

手順

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

ステップ 2 リモート クラスタと証明書を同期するには、[強制同期（Force Sync）] を選択します。

ステップ 3 表示される確認ウィンドウで、[ピアの Tomcat 証明書も再同期（Also resync peer's Tomcat certificates）] を選択します。

ステップ 4 [OK] をクリックします。

（注） 自動的に同期しなかった証明書がある場合は、[クラスタ間ピアの設定（Intercluster Peer Configuration）] ウィンドウに移動します。x のマークが付けられたすべての証明書が存在していないため、手動でコピーする必要があります。

第 III 部

機能設定

第 11 章

IM and Presence Service 設定の可用性とインスタント メッセージ

IM and Presence Service の可用性の設定

IM and Presence サービス クラスタのプレゼンス ステータス共有のオン/オフ

この手順では、IM and Presence Service クラスタのすべてのクライアント アプリケーションにおけるプレゼンス ステータス共有をオンまたはオフにする方法について説明します。

プレゼンス ステータス共有は、IM and Presence Service でデフォルトでオンになっています。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）] を選択します。

ステップ 2 プレゼンス ステータスを設定します。次のいずれかの操作を実行します。

- IM and Presence Service クラスタでのプレゼンス ステータス共有をオンするために、[プレゼンス ステータス共有の有効化（Enable availability sharing）] のチェックボックスをオンにしてください。この設定をオンにすると、IM and Presence Service では、ユーザのポリシー設定に基づいて、クラスタ内のすべてのユーザ間でそのユーザのプレゼンス ステータス情報が共有されます。

  ユーザのデフォルトのポリシー設定では、他のすべてのユーザがそのプレゼンス ステータスを表示できます。ユーザは、Cisco Jabber クライアントから、ポリシー設定をします。

- IM and Presence Service クラスタですべてのクライアントのプレゼンス ステータス共有をオフするために、[Eプレゼンス ステータス共有の有効化（nable availability sharing）] のチェックボックスをオフにしてください。この設定をオフにすると、IM and Presence Service では、IM and Presence Service クラスタ内の他のユーザとプレゼンス ステータスが共有されません。また、クラスタ外から受信したプレゼンス ステータス情報も共有されません。ユーザは自分のプレゼンス ステータスだけを表示できます。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 次のサービスを再起動します。

a) Cisco XCP Router
b) Cisco Presence Engine

ヒント
- プレゼンス ステータス共有をオフにすると、ユーザは、クライアント アプリケーションで自分のプレゼンス ステータスを表示できます。その他のすべてのユーザのプレゼンス ステータスはグレー表示されます。
- プレゼンス ステータス共有をオフにして、ユーザがチャットルームに入ると、そのプレゼンス ステータスは、緑色のアイコンで 「不明」 ステータスを示します。

一時的（アドホック）プレゼンス サブスクリプションの設定

（注） これらの設定で、ユーザ連絡先リストにないユーザに一時的（アドホック）プレゼンス 登録を開始できます。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）] を選択します。

ステップ 2 Cisco Jabber ユーザ用の一時的（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ために、[一時的（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（Enable ad-hoc presence subscriptions）] のチェックボックスをオンにします。

ステップ 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 サブスクリプション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 サブスクリプションを無制限に許可します。

ステップ 4 一時的（アドホック）プレゼンス サブスクリプションの存続可能時間値（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 サブスクリプションをドロップし、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） ユーザがまだ一時的（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 メッセージを表示し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ことがあります。

ステップ 5 [保存（Save）] をクリックします。
この設定のために IM and Presence Service のど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 の最新の一時的（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。

ユーザごとの連絡先リストの最大サイズの設定

ユーザの連絡先リストの最大サイズを設定できます。これはユーザが連絡先リストに追加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 の管理の [システム トラブルシューター（System Troubleshooter）] に表示されます。

IM and Presence Service にユーザを移行する場合は、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。これは移行された各ユーザ連絡先リストが完全にインポートされることを保障します。すべてのユーザが移行した後、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優先値にリセットできます。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] を選択します。

ステップ 2 [連絡先リストの最大サイズ（ユーザごと）（Maximum Contact List Size （per user））] 設定の値を編集します。
デフォルト値は 200 です。

ヒント 連絡先リストのサイズを無制限にするには、[無制限（No Limit）] チェックボックスをオンにします。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 Cisco XCP Router サービスを再起動します。

関連トピック

Cisco XCP ルータ サービスの再起動, （68 ページ）

ユーザごとの最大ウォッチャ数の設定

ユーザのウォッチャの数、特にユーザのプレゼンス ステータスを表示するために登録できるユーザの最大数を設定できます。この設定は、Cisco Jabber クライアントとサードパーティ クライアントの連絡先リストに適用されます。

IM and Presence Service にユーザを移行する場合は、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。これにより、移行した各ユーザ連絡先リストが完全にインポートされます。すべてのユーザが移行した後、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優先値にリセットできます。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] を選択します。

ステップ 2 [ウォッチャの最大数（ユーザごと）（Maximum Watchers （per user））] 設定の値を編集します。デフォルト値は 200 です。

ヒント ウォッチャの無制限の監視を許可するには、[無制限 （No Limit）] チェックボックスをオンにします。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 Cisco XCP Router サービスを再起動します。

IM and Presence Service の IM 設定

IM and Presence Service クラスタのインスタント メッセージのオン/オフ

この手順では、IM and Presence Service クラスタのすべてのクライアント アプリケーションにおけるインスタント メッセージ機能をオンまたはオフにする方法について説明します。インスタント メッセージ機能は、IM and Presence Service でデフォルトでオンになっています。

注意 IM and Presence Service のインスタント メッセージ機能をオフにすると、すべてのグループ チャット機能（アドホックおよびパーシステント チャット）が IM and Presence Service で動作しません。Cisco XCP Text Conference サービスをオンにしないか、IM and Presence Service のパーシステント チャットの外部データベースを設定しないことを推奨します。

手順

ステップ 1 **Cisco Unified CM IM and Presence Administration** にログインし、[メッセージング（Messaging）] > [設定（Settings）] を選択します。

ステップ 2 インスタント メッセージングを設定します。次のいずれか 1 つの処理を実行します。

- IM and Presence Service クラスタのクライアント アプリケーションにおけるインスタント メッセージ機能をオンにするには、[インスタント メッセージを有効にする（Enable instant messaging）] のチェックボックスをオンにします。この設定をオンにすると、クライアント アプリケーションのローカル ユーザはインスタント メッセージを送受信できます。
- IM and Presence Service クラスタのクライアント アプリケーションにおけるインスタント メッセージ機能をオフにするには、[インスタント メッセージを有効にする（Enable instant messaging）] のチェックボックスをオフにします。

  （注） この設定をオフにすると、クライアント アプリケーションのローカル ユーザはインスタント メッセージを送受信できません。ユーザは、プレゼンス ステータスおよび電話操作にのみインスタント メッセージ アプリケーションを使用できます。この設定をオフにすると、ユーザはクラスタの外部からインスタント メッセージを受信しません。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 Cisco XCP Router サービスを再起動します。

オフライン インスタント メッセージのオン/オフ

デフォルトでは、IM and Presence サービスはユーザがオフラインのときにユーザに送信されたインスタントメッセージを（ローカルに）保存し、ユーザが次にクライアントアプリケーションにサインインしたときに、IM Presence サービスはこれらのインスタントメッセージをユーザに配信します。この機能をオフに（抑制）して、IM and Presence サービスがオフライン インスタント メッセージを保存しないようにすることができます。

（注） IM and Presence サービスはオフライン メッセージを 1 ユーザあたり 100 個、1 ノードあたり最大 30000 個に制限します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [メッセージング（Messaging）] > [設定（Settings）] を選択します。

ステップ 2 オフライン インスタント メッセージングを設定します。次のいずれかの操作を実行します。

- IM and Presence サービスのオフライン インスタント メッセージ のストレージをオフにするには、[オフライン インスタント メッセージの抑制（Suppress Offline Instant Messaging）] のチェックボックスをオンにします。この設定をオンにすると、IM and Presence サービス はユーザがオフラインのときにユーザに送信されたインスタント メッセージを、ユーザが次にクライアント アプリケーションにサインインしたときにユーザに配信しません。
- IM and Presence サービスのオフライン インスタント メッセージのストレージをオンにするには、[オフライン インスタント メッセージの抑制（Suppress Offline Instant Messaging）] のチェックボックスをオフにします。この設定をオフにすると、IM and Presence サービス はユーザがオフラインのときにユーザに送信されたインスタント メッセージを、ユーザが次にクライアント アプリケーションにサインインしたときにユーザに配信します。

ステップ 3 [保存（Save）]をクリックします。

インスタントメッセージでのカットアンドペーストの許可

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

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [メッセージング（Messaging）] > [設定（Settings）] を選択します。

ステップ 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 サービスでインスタント メッセージ履歴のログ記録を許可する場合は、[クライアントでインスタント メッセージ履歴のログ記録を許可（サポートされるクライアントでのみ）（Allow clients to log instant message history（on supported clients only））] をオンにしてください。
- クライアントアプリケーションのユーザに IM and Presence サービスでインスタント メッセージ履歴のログ記録を許可しない場合は、[クライアントでインスタント メッセージ履歴のログ記録を許可（サポートされるクライアントでのみ）（Allow clients to log instant message history（on supported clients only））] をオフにしてください。

ステップ 3 [保存（Save）]をクリックします。

インスタント メッセージでのカット アンド ペーストの許可

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

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [メッセージング（Messaging）] > [設定（Settings）] を選択します。

ステップ 2 次のようにインスタント メッセージでのカット アンド ペーストの設定を行います。

- インスタント メッセージでカット アンド ペーストすることをクライアント アプリケーションのユーザに許可する場合は、[インスタント メッセージのカット アンド ペーストの許可（Allow cut & paste in instant messages）] をオンにします。
- インスタント メッセージでカット アンド ペーストすることをクライアント アプリケーションのユーザに許可しない場合は、[インスタント メッセージのカット アンド ペーストの許可（Allow cut & paste in instant messages）] をオフにします。

ステップ 3 [保存（Save）] をクリックします。

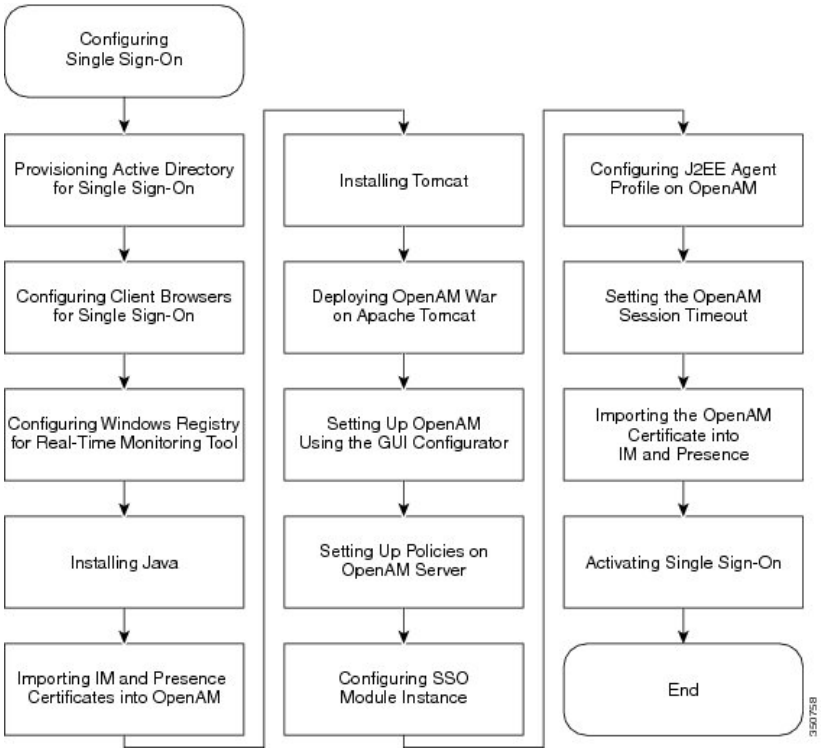
第 12 章

OpenAM シングル サインオン

シングル サインオン設定のタスクリスト

次の図は、正常に SSO を設定するために必要なタスクの手順について説明します。この順序どおりに、このフローで説明している各タスクを実行することを推奨します。

図 *12*：シングル サインオン設定のタスク フロー



次の表は、シングル サインオンを設定するタスクを示します。

表 *19*：シングル サインオン設定のタスク リスト

項目	タスク
1	Active Directory（AD）サーバの シングル サインオンを使用する OpenAM サーバの新しいユーザ アカウントをプロビジョニングします。 （注） 先に進む前に、Windows Server 2008 のサポート ツールがインストールされていることを確認してください。
2	シングル サインオンのためにクライアント ブラウザを設定します。サードパーティ製ソフトウェア、Web ブラウザのリストのシステム要件、およびサポート対象のバージョンの関連トピックを参照してください。

項目	タスク
3	Real-Time Monitoring Tool（RTMT）用の Microsoft Windows レジストリを設定します。
4	Java Runtime Environment（JRE）をインストールします。 （注） Java キー ストアと関連セキュリティ証明書は Apache Tomcat で動作する OpenAM サーバへのセキュア接続が必要になります。Java をインストールする手順は、自己署名されたセキュリティ証明書を使用するか、または、証明局（CA）によって署名されたセキュリティ証明書を使用するかによって異なります。
5	OpenAM に IM and Presence サービス証明書をインポートします。シングル サインオンを使用するための、各 IM and Presence サービス ノードに対してこの作業を実行します。
6	OpenAM Windows サーバで Apache Tomcat Web Container をインストールします。
7	Apache Tomcat で OpenAM War を展開します。
8	GUI Configurator を使用して OpenAM をセットアップします。OpenAM サーバの FQDN を入力することで、Web ブラウザを使用する OpenAM web ベースの管理インターフェイスにアクセスします。
9	OpenAM サーバのポリシーの設定この手順で定義されるポリシー規則に従う必要があります。 （注） Cisco Unified CM IM and Presenceの管理/ユーザ インターフェイスにアクセスするには、IM and Presence サービス ノードの FQDN を使用する必要があります。ノードのホスト名を使用しないでください。
[10]	SSO モジュール インスタンスを設定します。同じ Active Directory ドメインが展開全体で使用される場合、単一モジュール インスタンスを、SSO の複数の IM and Presence サービス ノードによって共有できます。
11	OpenAM の J2EE Agent プロファイルを設定します。SSO を使用する各 IM and Presence サービス ノードの J2EE エージェント用の OpenAM サーバの関連 J2EE Agent プロファイルを設定する必要があります。
12	OpenAM セッション タイムアウトを IM and Presence サービス ノードのセッション タイムアウト パラメータ設定よりも大きい値に設定します。
13	SSO を使用して各 IM and Presence サービス ノード の tomcat-trust の信頼ストアに OpenAM 証明書をインポートします。

項目	タスク
18	シングル サイン オンのアクティブ化 **注意** SSO を有効にすると、サービスに影響を与えます。メンテナンス時間枠の間に、SSO を有効にすることを強く推奨します。

シングル サインオンのセットアップ時に必要のない次の追加タスクを実行できます。

- シングル サイン オンの無効化
- Windows での OpenAM のアンインストール
- デバッグ レベルの設定
- シングル サインオンのトラブルシューティング

関連トピック

シングル サイン オンの無効化, （195 ページ）
Windows での OpenAM のアンインストール, （195 ページ）
デバッグ レベルの設定, （196 ページ）
シングル サインオンのトラブルシューティング

シングル サインオン設定の準備

シングル サインオンでのサードパーティ製ソフトウェアとシステムの要件

シングル サインオン（SSO）機能では、OpenAM と呼ばれる ForgeRock のサードパーティ製アプリケーションを使用します。OpenAM アプリケーションのサポートは、ForgeRock のみから利用できます。SSO 機能を OpenAM と連動できるようにするために、ソフトウェア要件と設定ガイドラインが提供されています。Windows Server での OpenAM のインストールについても、説明されています。

ロードバランサの背後での OpenAM の展開や、OpenAM サーバ間でのセッション レプリケーションの使用などの、OpenAM の高度な設定は検証されていません。これらの高度な機能の詳細については、http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf を参照してください。

SSO 機能には、次のサードパーティ製アプリケーションが必要です。

- Microsoft Windows Server 2008 R2
- Microsoft Active Directory
- ForgeRock Open Access Manager（OpenAM）バージョン 9.0

（注） SSO 機能は、Active Directory と OpenAM を組み合わせて使用することにより、Web ベースのクライアント アプリケーションへの SSO アクセスを提供します。

これらのサードパーティ製品は、次の設定要件を満たす必要があります。

- Active Directory は、LDAP サーバとしてではなく、Windows ドメインベースのネットワーク設定で導入される必要があります。
- OpenAM サーバは、ネットワーク上のすべてのクライアント システムおよび Active Directory サーバからアクセスできる必要があります。
- Active Directory（ドメイン コントローラ）サーバ、Windows クライアント、IM and Presence Service、および OpenAM サーバは、同じドメイン内に存在する必要があります。
- DNS をドメイン内で有効にする必要があります。
- SSO に参加するすべてのエンティティのクロックを同期させる必要があります。

サードパーティ製品の詳細については、各製品のマニュアルを参照してください。

次の表は、この章に示されている手順で使用され、テストされたソフトウェア アプリケーションとバージョンのリストです。シスコのサポートを受けるには、シスコは設定時にこれらの推奨要件に従うことを推奨します。

表 *20*：ソフトウェア バージョン

コンポーネント	バージョン
Active Directory	Windows Server 2008 R2 Enterprise
エンド ユーザ クライアント用のデスクトップ オペレーティング システム	Windows 7 Professional（SP1）
OpenAM	OpenAM Release 10.0 http://forgerock.org/openam-archive.html 詳細については、次を参照してください。 https://wikis.forgerock.org/confluence/display/openam/OpenAM+Release+Documentation
OpenAM の基盤となるオペレーティング システム	Windows Server 2008 R2 Enterprise
OpenAM のロード先の Apache Tomcat	Tomcat 6.0.2.0、Tomcat 7.0.29 http://archive.apache.org/dist/tomcat/tomcat-7/v7.0.29/bin

コンポーネント	バージョン
OpenAM の Java Development Kit（JDK）の基盤となるオペレーティング システム	JDK 7 アップデート
Web ブラウザ	Internet Explorer 8、9、および Mozilla Firefox 10、11

シングル サインオンの設定前の重要な情報

（注） Release 10.0(1) 以降、エージェントのフロー SSO は FIPS モードとの互換性がありません。

SSO の設定が可能な限り円滑に動作するよう、SSO を設定する前に次の情報を収集することを推奨します。

- OpenAM システムのインストール ベースのオペレーティング システム（Windows サーバなど）が動作していることを確認します。
- OpenAM が統合される Windows Active Directory（AD）サーバの完全修飾ドメイン名（FQDN）を書き留めます。
- OpenAM をインストールする Windows サーバの FQDN を書き留めます。
- IM and Presence Web アプリケーションのタイムアウトが、クラスタ内のすべての IM and Presence ノード間で一貫して設定されていることを確認し、そのタイムアウト値を書き留めます。Cisco Unified CM IM and Presence の管理 CLI を使用して、show webapp session timeout コマンドを入力し、タイムアウト値を確認します。詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。
- 「sAMAccountName」をユーザ ID の LDAP 属性として使用して、Active Directory（AD）からユーザを同期するように Cisco Unified Communications Manager が設定されていることを確認します。詳細については、『*Cisco Unified Communications Manager System Guide*』の「DirSync サービス」の章を参照してください。

シングル サインオンの設定と管理のタスク

シングル サインオンの **Active Directory** のプロビジョニング

はじめる前に

Windows Server 2008 がインストールされたツールをサポートすることを確認します。サポートツールは、Windows Server 2008 にデフォルトでインストールされています。

手順

ステップ 1 Active Directory（AD）サーバにログインします。

ステップ 2 [開始（Start）] メニューで、[プログラム（Programs）] > [管理ツール（Administration Tools）] を選択し、[アクティブ ディレクトリ ユーザとコンポーネント（Active Directory Users and Computers）] を選択します。

ステップ 3 [ユーザ（Users）] を右クリックし、[新規（New）] > [ユーザ（User）] を選択します。

ステップ 4 [ユーザ ログイン名（User logon name）] フィールドに、「OpenAM サーバのホスト名」を入力します。

（注） OpenAM サーバ のホスト名にドメイン名を含めることはできません。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 パスワードを入力し、確認します。
このパスワードはステップ 10 で必要です。

ステップ 7 [ユーザは次のログイン時に変更する必要があります（User Must Change at Next login）] チェックボックスをオフにします。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 新しいユーザ アカウントの作成を終了するには、[完了（Finish）] をクリックします。

ステップ 10 コマンド プロンプトから次のコマンドを使用して、AD サーバの keytab ファイルを作成します。

```
ktpass -princ HTTP/<hostname>.<domainname>@<DCDOMAIN> -pass <password> -mapuser <userName>
 -out <hostname>.HTTP.keytab -ptype KRB5_NT_PRINCIPAL -target <DCDOMAIN>
```

例：

```
ktpass -princ HTTP/server1.cisco.com@CISCO.COM -pass cisco!123 -mapuser server1 -out
server1.HTTP.keytab -ptype KRB5_NT_PRINCIPAL -target CISCO.COM
```

引数の説明

パラメータ	説明
hostname	OpenAM サーバのホスト名（FQDN ではなく）。たとえば、server1
domainname	AD ドメイン名。たとえば、cisco.com。
DCDOMAIN	印刷字体の大文字で入力される AD ドメイン名。この例では、CISCO.COM。
password	この前の手順で OpenAM サーバのユーザ アカウントを作成したときに指定したパスワード値。
userName	ステップ 4 で入力した AD アカウント名。この値は OpenAM サーバのホスト名である必要があります。この例では、server1。

（注） 後の手順で使用するため *-princ* 値を記録します。

ステップ 11 keytab ファイルが正常に作成されたら、OpenAM サーバの場所に keytab ファイルをコピーします。このパスは、後で OpenAM 設定で指定します。ディレクトリを `C:\>` の下に作成して、上記のキータブ ファイルをコピーします。たとえば、`C:/keytab/server1.HTTP.keytab`。

シングル サインオン用のクライアント ブラウザ設定

ブラウザベースのクライアント アプリケーションに SSO を使用する場合は、Web ブラウザを設定する必要があります。ここでは、SSO を使用するようにクライアント ブラウザを設定する方法について説明します。

シングル サインオン用の Internet Explorer の設定

SSO 機能は、Internet Explorer を実行している Windows クライアントをサポートします。SSO を使用するために Internet Explorer を設定するには、次の手順を実行します。

ヒント サポートされる Web ブラウザの詳細については、サードパーティ製ソフトウェアとシングル サインオンのシステム要件に関連するトピックを参照してください。

手順

ステップ 1 [ツール（Tools）] > [インターネット オプション（Internet Options）] > [詳細（Advanced）] タブを選択します。

ステップ 2 [統合 Windows 認証を有効にする（Enable Integrated Windows Authentication）] をオンにします。

ステップ 3 [OK] をクリックして変更を保存します。

ステップ 4 Internet Explorer を再起動します。

ステップ 5 [ツール（Tools）] > [インターネット オプション（Internet Options）] > [セキュリティ（Security）] >[ローカルイントラネット（Local Intranet）] を選択し、[レベルのカスタマイズ（Custom Level）] をクリックします。

ステップ 6 [ユーザ認証（User Authentication）] で、[イントラネット ゾーンでのみ自動的にログオンする（Automatic Logon Only in Intranet Zone）] を選択します。

ステップ 7 [OK] をクリックします。

ステップ 8 [サイト（Sites）] をクリックします。

ステップ 9 [イントラネットのネットワークを自動的に検出する（Automatically detect intranet network）] をオンにします。

ステップ 10 [詳細設定（Advanced）] をクリックします。

ステップ 11 [この Web サイトをゾーンに追加する（Add this web site to the zone）] フィールドに、OpenAM サーバの FQDN を https://OpenAM_FQDN の形式で入力します。

ステップ 12 [追加（Add）] をクリックします。

ステップ 13 [閉じる（Close）] をクリックします。

ステップ 14 [OK] をクリックします。

ステップ 15 [保護モードを有効にする（Enable Protected Mode）] をオフにします。

ステップ 16 [適用（Apply）] をクリックします。

ステップ 17 [OK] をクリックします。

ステップ 18 Internet Explorer を再起動します。

ステップ 19 Windows レジストリ エディタを開きます。次のいずれかの操作を実行します。

- Windows XP または Windows 2008 では、[開始（Start）]> [実行（Run）] を選択し、「*regedit*」と入力します。
- Windows Vista および Windows 7.0 では、[開始（Start）] をクリックし、「*regedit*」と入力します。Windows Vista では、[継続（Continue）] をクリックする必要があります。

ステップ 20 登録キー [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\] の下の [新規（New）] > [DWORD（32 ビット）値（NewDWORD（32-bit）value）] を右クリックして、選択し、*SuppressExtendedProtection* に名前を変更します。
管理者のみ DWORD を設定できます。

ステップ 21 次の値を設定します。

- [表記（Base）] : [16 進（hexadecimal）]

- [値のデータ（Value data）]：002

新しく作成された DWORD は、LSA ディレクトリ リストに次のように表示されます。

- Name: SuppressExtendedProtection
- Type: REG_DWORD
- Value: 0x00000002 (2)

関連トピック

シングル サインオンでのサードパーティ製ソフトウェアとシステムの要件, （160 ページ）

シングル サインオン用の Firefox の設定

SSO 機能は、Firefox を実行する Windows クライアントをサポートしています。

ヒント　サポートされている Web ブラウザの一覧については、「サードパーティ製ソフトウェアとシングル サインオンのシステム要件」に関するトピックを参照してください。

手順

ステップ 1　Firefox を開き、次の URL を入力します。**about:config**

ステップ 2　[network.negotiate-auth.trusted-uris] へスクロール ダウンし、[プリファレンス名（Preference Name）] を右クリックし、[変更（Modify）] を選択します。

ステップ 3　ドメイン（たとえば、cisco.com）に文字列値を設定します。

ステップ 4　[OK] をクリックします。

関連トピック

シングル サインオンでのサードパーティ製ソフトウェアとシステムの要件, （160 ページ）

Real-Time Monitoring Tool（RTMT）用の Windows レジストリ設定

Real-Time Monitoring Tool（RTMT）用の SSO 設定は任意です。この設定を実現するには、デスクトップ クライアントの新しいレジストリ キーを作成する必要があります（Windows XP または Windows 7）。

（注） 管理者は、デスクトップ クライアント用の「`allowtgtsessionkey`」レジストリ キー エントリを設定する必要があります。

この新しいレジストリ キーは、オペレーティング システムに応じて、次の場所のいずれかに保存します。

手順

ステップ 1 使用するオペレーティング システムに応じて、次の場所のいずれかに移動します。

- Windows XP：`HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Control \ Lsa \ Kerberos`
- Windows Vista/Windows 7：`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters`

ステップ 2 フォルダを右クリックし、[新規（New）]>[DWORD（32-ビット）値（DWORD（32-bit）Value）] を選択し、「*allowtgtsessionkey*」に名前を変更します。

ステップ 3 新しく作成されたレジストリ キーを右クリックし、[変更（Modify）] を選択します。

ステップ 4 [値のデータ（Value data）] フィールドに、「I」と入力します。

Java のインストール

OpenAM は Java Runtime Environment（JRE）が動作している必要があります。次の手順は、OpenAM ベースのシステムを形成する Windows サーバに JRE をインストールするための詳細を提供します。

手順

ステップ 1 http://www.oracle.com/technetwork/java/archive-139210.html に進みます。

ステップ 2 サーバ アーキテクチャ（Windows x86 または Windows x64）に対応する実行ファイル選択して、JDK のインストール ファイルの推奨バージョンをダウンロードします。

（注） 推奨されるソフトウェアのバージョンの一覧については、シングル サインオンのサードパーティ製ソフトウェアのシステム要件に関連したトピックを参照してください。

ステップ 3 ダウンロードしたファイルをダブルクリックして、JDK のインストールを開始し、インストール ウィザードで提供されるデフォルト値を受け入れます。

（注） インストールディレクトリを書き留めてください。この値は、Java JRE の位置を示し、JDK のディレクトリ パスを判断するために使用できます。使用される JDK 値に応じて、サンプルの値は次のようになります。

- `jre-path=C:\Program Files\Java\jre7`

- `jdk-path=C:\Program Files\Java\jdk1.7.0_03`

ステップ 4 Java キー ストアと関連付けられたセキュリティ証明書は、Apache Tomcat で動作する OpenAM サーバへのセキュア接続を容易にするために必要とされます。次のいずれかの操作を実行します。

- OpenAM/Tomcat の自己署名セキュリティ証明書を使用する場合は、ステップ 5 に進みます。
- OpenAM/Tomcat の認証局（CA）署名付きセキュリティ証明書を使用する場合は、ステップ 11 に進みます。

ステップ 5 Windows サーバ の Windows コマンド プロンプトを開くことによって、また、コマンドを実行することによってJavaキーストアを作成します。実行するコマンドは次のとおりです。`C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -genkey -alias tomcat -keyalg RSA -validity 1825 -keystore C:\keystore`
このコマンドは、`C:\keystore` に Java キーストア ファイルを作成します。keytool コマンドは、<jdk-path>/bin ディレクトリにあり、上記のコマンドの keytool コマンドへの正確なパスは使用される JDK のバージョンによって異なる場合があります。keytool コマンドの詳細については、http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html を参照してください。

ステップ 6 キーストア パスワードを入力するよう求められたら、有効なキーストア パスワードを入力します。たとえば、「cisco!123」などです。キーストアにアクセスする必要があるので、キーストア パスワードを書き留めておいてください。

（注） 実稼働サーバで値の例を使用せず、キーストアの固有のパスワード値を使用してください。このパスワードは、Apache Tomcat コンフィギュレーション ファイルおよびユーティリティのプレーン テキストで表示されます。

ステップ 7 名および姓を入力するよう求められたら、OpenAM サーバの FQDN （hostname.domainname）を入力します。
また、組織ユニット名、組織名、市または地域、都道府県、および 2 文字の国番号を入力するよう求められます。

ステップ 8 Tomcat パスワードを入力するよう求められたら、Tomcat プライベート キーに同じキー ストアのパスワードを使用するには、[Return] キーを押します。Java キーストアは keytool コマンドで指定された場所に作成されます。たとえば、`C:\keystore` です。

ステップ 9 次のコマンドを使用して、キーストアの Tomcat 証明書を表示できます。

例：
```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -list -v -alias tomcat -keystore
C:\keystore
```

ステップ 10 *Tomcat* の自己署名セキュリティ証明書を選択する場合は、この手順の最後に進み、このタスクを実行を検討してください。

ステップ 11 OpenAM/Tomcat の認証局（CA）署名のセキュリティ証明書を保存するために Java キーストアを作成します。Windows サーバでコマンド プロンプトを開き、次のコマンドを実行します。

例：
```
C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -genkey -alias tomcat -keyalg RSA
-validity 1825 -keystore C:\keystore
```

このコマンドは、C:\keystore に Java キーストア ファイルを作成します。keytool コマンドは、<jdk-path>/bin ディレクトリにあり、上記の例の keytool コマンドへの正確なパスは使用される JDK のバージョンによって異なる場合があります。keytool コマンドの詳細については、http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html を参照してください。

ステップ 12 キーストア パスワードを入力するよう求められたら、有効なキーストア パスワードを入力します。たとえば、「cisco!123」などです。キーストアにアクセスする必要があるので、キーストア パスワードを書き留めておいてください。
実稼働サーバで値の例を使用せず、キーストアの固有のパスワード値を使用してください。このパスワードは、Apache Tomcat コンフィギュレーション ファイルおよびユーティリティのプレーン テキストで表示されます。

ステップ 13 名および姓を入力するよう求められたら、OpenAM サーバの FQDN（hostname.domainname）を入力します。
また、組織ユニット名、組織名、市または地域、都道府県、および 2 文字の国番号を入力するよう求められます。

ステップ 14 Tomcat パスワードを入力するよう求められたら、Tomcat プライベート キーに同じキー ストアのパスワードを使用するには、[Return] キーを押します。Java キーストアは keytool コマンドで指定された場所に作成されます。たとえば、`C:\keystore` です。

ステップ 15 次のコマンドを使用して、キーストアの Tomcat 証明書を表示できます。

例：

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v -alias tomcat -keystore
C:\keystore
```

ステップ 16 OpenAM/Tomcat インスタンスの証明書署名要求（CSR）を生成します。Windows サーバでコマンド プロンプトを開き、次のコマンドを実行します。

例：

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -certreq -keyalg RSA -alias tomcat
-file certreq.csr -keystore C:\keystore
```

ステップ 17 CSR を CA に送信し、CSR に署名し、証明書を作成することを CA に要求します。OpenAM サーバとなる Windows サーバに次の証明書を取得し、コピーします。

- CA の署名またはルート証明書
- 中間署名証明書（該当する場合）
- 最新の署名付き OpenAM/Tomcat 証明書

（注） これらのタスクを完了する手順については、CA のマニュアルを参照してください。

ステップ 18 ステップ 11 で作成された Java キー ストアに CA の署名またはルート証明書をインポートします。Windows サーバでコマンド プロンプトを開き、「この証明書を実行しますか」というプロンプトに「はい（yes）」と応答する次のコマンドを実行します。

例：

```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -import -alias
root -trustcacerts -file <filename_of_the_CA_root_certificate> -keystore
C:\keystore
```

ステップ 19 次のコマンドを使用して、キーストアの CA 署名の証明書を検索できます。

例：
```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v -alias
root -keystore C:\keystore
```

ステップ 20 ステップ 11 で作成された Java キーストアに他の中間署名証明書（該当する場合）をインポートします。Windows サーバでコマンド プロンプトを開き、「この証明書を実行しますか」というプロンプトに「はい（yes）」と応答する次のコマンドを実行します。

例：
```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -import -alias
inter01 -trustcacerts -file
<filepath_of_the_intermediate_signing_certificate> -keystore C:\keystore
```
- alias オプションを Java キーストアに固定の値で更新する必要があります。そうしない場合、インポート操作は「インポートされていない証明書は、alias<inter01> はすでに存在します」のようなエラーになります。

ステップ 21 次のコマンドを使用してキーストアの中間署名証明書を表示できます。

例：
```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v -alias
inter01 C:\keystore
```
-alias オプションを表示する中間証明書の対応するエイリアス値で更新する必要があります。上記の例は、「inter01」のサンプル エイリアス値を使用します。

ステップ 22 ステップ 11 で作成された Java キーストアに最新の署名付き証明書の OpenAM/tomcat 証明書をインポートします。Windows サーバでコマンド プロンプトを開き、次のコマンドを実行します。

例：
```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -import -alias
tomcat -file <new_certificate_filepath> -keystore C:\keystore
```

ステップ 23 次のコマンドを使用して、キーストアの新しい OpenAM/Tomcat 証明書を表示できます。

例：
```
C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keytool.exe" -list -v -alias
tomcat -keystore C:\keystore
```
この新しい tomcat 証明書の発行者は CA または中間 CA の 1 つです（該当する場合）。

関連トピック

シングル サインオンでのサードパーティ製ソフトウェアとシステムの要件, （160 ページ）
IM and Presence サービスへの OpenAM 証明書のインポート, （186 ページ）

OpenAM への IM and Presence 証明書のインポート

OpenAM は SSO が有効に設定された各 IM and Presence サービス ノードに存在する J2EE エージェント コンポーネントと通信する必要があります。この通信は暗号化されたチャネル経由であるため、必要なセキュリティ証明書を OpenAM にインポートする必要があります。

OpenAM サーバは確立される暗号化された通信チャネルの各 IM and Presence サービス ノードが提示するセキュリティ証明書を信頼する必要があります。OpenAM は OpenAM キーストアへ必要なセキュリティ証明書をインポートすることでセキュリティ証明書を信頼します。特定の IM and Presence サービス ノードは、セキュリティ証明書の 2 種類うち 1 つを提示できます。

- 自己署名証明書
- CA-signed 証明書

（注） IM and Presence サービスの Tomcat 証明書と tomcat-trust の信頼ストアは OpenAM のセキュア通信のためのセキュリティ証明書が含まれます。他の IM and Presence サービスの証明書と関連する信頼ストアは SSO には関連しません（たとえば、cup、cup-xmpp、cup-xmpp-s2s または ipsec）。

自己署名証明書を使用するように SSO 対応の IM and Presence サービス展開を設定する場合は、自己署名証明書をそれぞれ、OpenAM にインポートする必要があります。

CA 署名付き証明書を使用するように SSO 対応の IM and Presence サービス展開が設定される場合は、CA ルート証明書および関連する中間証明書を OpenAM にインポートする必要があります。また OpenAM/Tomcat インスタンスに CA 署名付き証明書を使用する場合も、要求される CA ルート証明書および中間証明書は OpenAM キーストアにすでにインポートされている可能性があります。

この手順は、Java をインストールした時に、IM and Presence サービス ノードによって使用されるセキュリティ証明書のタイプを識別する方法と、作成された OpenAM キーストアに証明書をインポートする方法の詳細を提供します。

手順

ステップ 1 SSO 対応の IM and Presence サービス ノードの 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。

ステップ 2 [セキュリティ（Security）] > [証明書管理（Certificate Management）] を選択します。

ステップ 3 [検索（Find）] をクリックします。

ステップ 4 Tomcat の証明書の名前のエントリを見つけます。

ステップ 5 Tomcat 証明書の[説明（Description）] 列を確認します。

ステップ 6 説明が、Tomcat 証明書はシステムによって生成された自己署名証明書であることを示す場合は、IM and Presence サービス ノードが自己署名証明書を使用していることを示します。この説明がない場合、CA 署名付き証明書が使用できます。

- 自己署名証明書の場合は、ステップ 7 に進みます。
- CA 署名付き証明書の場合は、ステップ 13 に進みます。

ステップ 7 [tomcat.pem（tomcat.pem）] リンクをクリックします。

ステップ 8 tomcat.pem ファイルをダウンロードするには、[ダウンロード（Download）] をクリックします。

ステップ 9 OpenAM サーバに tomcat.pem ファイルをコピーします。

ステップ 10 Java をインストールした時に、OpenAM サーバで作成されるキーストアに信頼できる証明書として tomcat.pem ファイルをインポートします。Windows サーバ（OpenAM）でコマンド プロンプトを開き、次のコマンドを実行します。環境に合わせて keytool コマンドのパスとキーストアの場所の値のコマンドを更新するには、「この証明書を信頼しますか」というプロンプトに「はい（yes）」と応答します。 `C:\>"C:\Program Files\Java\jdkl.7.0_03\bin\keystool.exe" -import -alias cup01 -trustcacerts -file <full_filepath_of_the_tomcat.pem> -keystore C:\keystore`

（注） - alias オプションは Java キー ストアに固有の値で更新する必要があります。そうでない場合は、インポート操作が次のようなエラーになる可能性があります。「インポートされていない証明書、alias <cup01> はすでに存在します」

ステップ 11 環境に合わせて keytool コマンドのパスとキーストアの場所の値を更新することで、次のコマンドを使用してキーストアの tomcat.pem を表示できます。
`C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keystool.exe -list -v -alias cup01 -keystore C:\keystore`

（注） - alias オプションは、ステップ 10 で使用する値に一致する必要があります。そうでない場合は、キーストア エントリが見つからない場合があります。

ステップ 12 ステップ 16 に進みます。

ステップ 13 IM and Presence サービス のTomcat 証明書の署名に使用された CA ルート証明書と中間証明書を識別します。CA から OpenAM サーバに必要な証明書（CA ルート証明書および中間証明書）をダウンロードします。

ステップ 14 信頼される証明書として OpenAM サーバのキーストアにこれらの証明書をインポートします。Windows サーバ（OpenAM）でコマンドプロンプトを開き、環境に合わせて keytool コマンドのパスとキーストアの場所の値のコマンドを更新することで、ダウンロードした証明書それぞれに次のコマンドを実行し、「この証明書を信頼しますか」というプロンプトに「はい（Yes）」と答えます。
`C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keytool.exe" -import -alias root_ca -trustcacerts -file <full_filepath_of_the_certificate> -keystore C:\keystore`

（注） - alias オプションは Java キー ストアに固定な値で更新する必要があります。そうでない場合は、インポート操作が次のようなエラーになる可能性があります。「インポートされていない証明書、エイリアス <root_ca> はすでに存在します」

ステップ 15 環境に合わせて keytool コマンドのパスとキーストアの場所の値を更新することで、次のコマンドを使用してキーストアの証明書を表示できます。
`C:\>"C:\Program Files\Java\jdk1.7.0_03\bin\keystool.exe -list -v -alias root_ca -keystore C:\keystore`

（注） - alias オプションは、ステップ 14 で使用する値に一致する必要があります。そうでない場合は、キーストア エントリが見つからない場合があります。

ステップ 16 SSO が有効に設定されている IM and Presence ノードそれぞれで、この手順を繰り返します。

（注） IM and Presence サービス ノードで使用される CA 署名付き証明書では、同じ CA 証明書と中間証明書をOpenAM キーストアに複数回インポートする必要はありません。IM and Presence サービス ノードが同じ CA 証明書および中間証明書によって署名されたことを検出する場合、OpenAM キーストアにそれらの証明書をインポートする必要はありません。

Tomcat のインストール

OpenAM では Apache Tomcat Web コンテナを OpenAM サーバ の Windows サーバ ベース のシステムにインストールする必要があります。この手順では、OpenAM Windows ベースのシステムでの Apache Tomcat のインストールの手順の詳細を説明します。この手順で参照される変数の説明については、次の表を参照してください。

表 *21*：変数の説明

変数	説明
<certstore-path>	Java アプリケーションと Apache Tomcat で使用される Java キーストアへのファイル パス。信頼できるサーバの公開証明書はこのキーストアに保存されます。Java キー ストアのファイル パスを設定するために次の手順のステップ 5 または 11 を参照してください。
<certstore-password>	<certstore-path> にある Java キーストアへのアクセスに使用するパスワード。Java キーストア パスワードに使用する値を設定するには、次の手順のステップ 6 または 12 を参照してください。

手順

ステップ 1 OpenAM ベース システムを構成する Windows サーバに Apache Tomcat の推奨バージョンをダウンロードします。推奨されるソフトウェアとバージョンの一覧については、シングル サインオンのサードパーティ製ソフトウェアとシステム要件に関するトピックを参照してください。

（注） 32bit/64bit Windows サービス インストーラの実行可能ファイルをダウンロードします。

ステップ 2 Apache Tomcat のインストールを開始するには、ダウンロードしたファイルをダブルクリックします。

ステップ 3 Apache Tomcat セットアップ ウィザードで [次へ（Next）] をクリックします。

ステップ 4 [ライセンス契約書（License Agreement）] ダイアログボックスで、[同意する（I agree）] をクリックします。

ステップ 5 [コンポーネントを選択（Choose Components）] ダイアログボックスで、インストールのタイプとして、[最少（Minimum）] をクリックして [次へ（Next）] を選択します。

ステップ 6 [設定（Configuration）] ダイアログボックスで、デフォルト設定に同意し、[次へ（Next）] をクリックします。

ステップ 7 [Java 仮想マシーン（Java Virtual Machine）] ダイアログボックスで、インストールされている JRE のパスが jre-path の値に設定されていることを確認します。

（注） Java の推奨バージョンを使用する場合、パスはデフォルトで表示されます。Java の推奨バージョンを使用しない場合は、入力したパスが Java のインストール時に使用されたパスに一致することを確認します。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 [インストール先の選択（Choose Install Location）] ダイアログボックスで、デフォルト設定を受け入れて、[インストール（Install）] をクリックします。後で必要になるので、Tomcat のインストール先を書き留めてください。

（注） インストール先は、この後の手順で「tomcat-dir」と呼ばれます。

ステップ 10 [終了（Finish）] をクリックします。

ステップ 11 自動的に起動するように Apache Tomcat を設定します。

a) [開始（Start）] > [すべてのプログラム（All Programs）] > [Apache Tomcat 7.0 Tomcat7（Apache Tomcat 7.0 Tomcat7）] > [Tomcat の設定（Configure Tomcat）] を選択します。

b) [全般（General）] タブで、[起動タイプ（Startup type）] を [自動（Automatic）] に設定します。

c) [適用（Apply）] をクリックします。

d) [OK] をクリックします。

ステップ 12 Apache Tomcat ランタイム パラメータを設定します。

a) [開始（Start）] > [すべてのプログラム（All Programs）] > [Apache Tomcat 7.0 Tomcat7（Apache Tomcat 7.0 Tomcat7）] > [Tomcat の設定（Configure Tomcat）] を選択します。

b) [Java] タブから、次の [Java オプション（Java options）] を追加します。

```
-Djavax.net.ssl.trustStore=<certstore-path>
-Djavax.net.ssl.trustStorePassword=<certstore-password>
-XX:MaxPermSize=256m
```

ヒント 変数の説明については、この手順の初めのパラメータ テーブルを参照してください。

例：

```
-Djavax.net.ssl.trustStore=C:\keystore
-Djavax.net.ssl.trustStorePassword=cisco!123
```

```
-XX:MaxPermSize=256m
```

c) [最初のメモリ プール（Initial memory pool）] を 512 に設定します。
d) [最大のメモリ プール（Maximum memory pool）] を1024 に設定します。
e) [適用（Apply）] をクリックします。
f) [OK] をクリックします。

ステップ 13 テキスト エディタを使用して、`<tomcat-dir>\conf` フォルダの下にある server.xml ファイルを開きます。<tomcat-dir> の値を設定するには、ステップ 9 を参照してください。

例：
値の例は「`C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf`」です。

ステップ 14 8080 コネクタ ポートをコメントにします。次のようにコードを入力します。

例：
```
<!-- <Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" /> -->
```

ステップ 15 8443 コネクタ ポートをアンコメントにします。8443 コネクタの最後の <!- - code at the beginning and - -> を削除します。コネクタの設定に、さらに 3 つの属性を追加する必要があります。

- keystoreFile（Java をインストールしたときに作成されたキーストア ファイルの場所。この例では、`C:\keystore` に作成されました）
- keystorePass
- keystoreType

次のようにコードを入力します。

例：
```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="<certstore-path>"
keystorePass="<certstore-password>"
keystoreType"JKS"/>
```

ヒント 変数の説明については、この手順の初めのパラメータ テーブルを参照してください。

ステップ 16 server.xml ファイルを保存します。

ステップ 17 Tomcat サービスを開始します。

a) [開始（Start）] > [すべてのプログラム（All Programs）] > [Apache Tomcat 7.0 Tomcat7（Apache Tomcat 7.0 Tomcat7）] > [Tomcat の設定（Configure Tomcat）]
b) [全般（General）] タブで [開始（Start）] をクリックします。Tomcat サービスがすでに実行されていた場合は、[停止（Stop）] をクリックし、次に [開始（Start）] をクリックします。

ステップ 18 設定をテストするには、Tomcat インスタンスを Windows サーバの Web ブラウザを開始し、`https://localhost:8443/tomcat.gif` にアクセスしてください。Web ブラウザが Tomcat

インスタンスによって表示されるセキュリティ証明書を信頼しないので、Webブラウザで非セキュアな接続に関する警告ダイアログが表示される場合があります。証明書を確認するか、ローカル証明書ストアに証明書を追加することで、ブラウザが証明書を信頼するか、使用可能なブラウザコントロールを使用してWebアプリケーション（より低いセキュア オプション）の手順を実行できます。設定が正しい場合、Tomcat ロゴは Web ブラウザ ウィンドウに表示されます。

ステップ 19 Apache Tomcat への着信接続を許可するために Windows ファイアウォールを設定します。

a) [開始（Start）] > [管理ツール（Administrative Tools）] > [Windows ファイアウォールおよびアドバンスド セキュリティ（Windows Firewall and Advanced Security）] を選択します。

b) [Windows ファイアウォールおよびアドバンスド セキュリティ（Windows Firewall and Advanced Security）] > [インバウンド ルール（Inbound Rules）] を選択します。

c) [インバウンド ルール（Inbound Rules）] を右クリックします。

d) [新しいルール（New Rule）] をクリックします。

e) [どのタイプのルールを作成しますか（What type of rule would you like to create）] オプションのリストで [ポート（Port）] を選択します。

f) [次へ（Next）] をクリックします。

g) [このルールをTCPまたはUDPに適用しますか（Does this rule apply to TCP or UDP?）] オプション リストで、[TCP] を選択します。

h) [このルールをすべてのローカル ポートまたは特定のローカル ポートに適用しますか（Does this rule apply to all local ports or specific local ports?）] オプションのリストで、[特定のローカル ポート（Specific local ports）] を選択します。

i) 「8443」を入力し、[次へ（Next）] をクリックします。

j) [接続が指定条件に一致する場合、どの操作をしますか（What action should be taken when a connection matches the specified conditions?）] オプションのリストで、[接続を許可（Allow the connection）] を選択します。

k) [次へ（Next）] をクリックします。

l) [いつルールを適用しますか（When does the rule apply?）] オプションのリストで、[ドメイン（Domain）] のみを選択します。

m) [次へ（Next）] をクリックします。

n) 選択する名前と説明を入力し、[終了（Finish）] をクリックします。

ステップ 20 設定をテストするには、ネットワークの別のホストにログインして、Tomcat インスタンスを含む Windows サーバの Web ブラウザを開始し、`https://<openam-fqdn>:8443/tomcat.gif` の Tomcat インスタンスを含む Windows サーバの完全修飾ドメイン名である `<openam-fqdn>` を参照します。 Web ブラウザが Tomcat インスタンスによって表示されるセキュリティ証明書を信頼しないので、Web ブラウザで非セキュアな接続に関する警告ダイアログが表示される場合があります。証明書を確認するか、ローカル証明書ストアに証明書を追加することで、ブラウザが証明書を信頼するか、使用可能なブラウザ コントロールを使用してWebアプリケーション（より低いセキュア オプション）の手順を実行できます。設定が正しい場合、Tomcat ロゴは Web ブラウザ ウィンドウにロードされ表示されます。

Apache Tomcat での OpenAM War の展開

手順

ステップ 1 ForgeRock の Web サイトから推奨される OpenAM リリースをダウンロードします。

ヒント 詳細については、シングル サインオンにおけるサードパーティ製ソフトウェアとシステム要件に関するトピックを参照してください。

ステップ 2 .zip ファイルを取得し、.zip ファイルに含まれる opensso.war ファイルを検索します。

ステップ 3 OpenAM サーバとなる Windows サーバに WAR ファイルをコピーします。この Windows サーバは、以前に設定された Tomcat サービスを実行する必要があります。

ステップ 4 Apache Tomcat サービスが実行中の場合は、Apache Tomcat サービスを停止します

a) [開始（Start）] > [すべてのプログラム（All Programs）] > [Apache Tomcat 7.0 Tomcat7（Apache Tomcat 7.0 Tomcat7）] > [Tomcat の設定（Configure Tomcat）] を選択します。

b) [全般（General）] タブで、[停止（Stop）] をクリックします。

ステップ 5 WAR ファイルを次の場所にコピーすることによって Tomcat インスタンスを含むWindows サーバの WAR ファイルを展開します。`<tomcat-dir>\webapps`

例：
`C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps`

（注） *<tomcat-dir>* 変数の説明については、Tomcat のインストールに関するトピックを参照してください。

ステップ 6 Apache Tomcat サービスを開始します。

a) [開始（Start）] > [すべてのプログラム（All Programs）] > [Apache Tomcat 7.0 Tomcat7（Apache Tomcat 7.0 Tomcat7）] > [Tomcat Tomcat7の設定（Configure Tomcat Tomcat7）] を選択します。

b) [全般（General）] タブで [開始（Start）] をクリックします。

（注） WAR ファイルは、数分以内に完全に展開されます。webapps フォルダに、WAR ファイルと同じ名前ではなく拡張子（.war）が削除された名前で新しいフォルダが作成されます。

ステップ 7 Web ブラウザを起動するか、または `https://<openam-fqdn>:8443/<war-file-name>` を入力して設定を確認します。そこでの *<openam-fqdn>* は、OpenAM/Tomcat インスタンスを含む Windows サーバの FQDN であり、*<war-file-name>* は拡張子（.war）が削除された OpenAM WAR ファイルの名前です。設定が正しい場合は、OpenAM 管理インターフェイスで Web ブラウザ ウィンドウがロードされます。

関連トピック

シングル サインオンでのサードパーティ製ソフトウェアとシステムの要件, （160 ページ）

GUI Configurator を使用した OpenAM のセットアップ

次の手順では、OpenAM の設定方法を指定します。既存の OpenAM サーバがある場合、または OpenAM について確実に理解している場合は、サーバを別に設定できます。

OpenAM サーバおよび J2EE Policy エージェントには、インストールを実行するマシンのホスト名の FQDN が必要です。インストール、設定、使用の問題が発生しないように、「localhost」のようなホスト名または「192.168.1.2」のような数字の IP アドレスの使用を避けることを強く推奨します。

OpenAM は Web ブラウザを使用してアクセスする必要がある、Mozilla Firefox などの Web ベースの管理インターフェイス を提供します。OpenAM に初めてアクセスする場合は、`https://server1.cisco.com:8443/opensso` などの URL で、OpenAM サーバの FQDN を使用する必要があります。このサンプルの URL 値では、OpenAM WAR ファイルが `opensso` として導入されることが想定されます。

OpenAM 設定およびロギング情報は OpenAM/Tomcat インスタンスを実行するユーザのホーム ディレクトリにある 2 つのディレクトリに通常保存されています。たとえば、

- `C:\opensso`（この場合、フォルダ名は OpenAM WAR ファイルのために展開される URI に一致します。たとえば、opensso）
- `C:\.openssocfg`

設定中に問題が発生した場合、コンフィギュレータはエラー メッセージを表示します。可能な場合は、エラーを修正して、設定をやり直します。次のログファイルディレクトリは役立つ情報を提供する場合があります。

- Tomcat Web コンテナのログ：`tomcat-dir\logs`
- OpenAM のインストール ログ： `C:\opensso`（フォルダ名は OpenAM WAR ファイルのために展開される URI に一致します。たとえば、opensso）

デフォルトでは、OpenAM は Windows プラットフォームの `C:\opensso` の下に展開されます。

手順

ステップ 1 Web ブラウザを開き、次の URL を使用して OpenAM サーバに移動します。`https://<fqdn of openam server>:8443/<WAR filename>`。

例：
`https://server1.cisco.com:8443/opensso`

（注） OpenAM に初めてアクセスするときは、OpenAM の初期設定を行うために Configurator に転送されます。OpenAM に初めてアクセスするときは、[設定オプション（Configuration Options）] ウィンドウが表示されます。

ステップ 2 [デフォルト設定の作成（Create Default Configuration）] を選択します。

（注） エラーが発生した場合は、ローカル マシンでステップ 1 と 2 を繰り返してください。

ステップ 3 [OpenSSO コンフィギュレータ（OpenSSO Configurator）] ウィンドウで、OpenAM 管理者（amAdmin）とデフォルト ポリシー エージェントのユーザ（UrlAccessAgent）のパスワードを指定し、確認します。デフォルト ポリシー エージェント ユーザは、この設定例では後で使用しません。amAdmin は、設定を変更するために OpenAM にログインするたびに使用します。

（注） amAdmin は OpenAM 管理者のみに適用される推奨値です。

ステップ 4 [構成の作成（Create Configuration）] をクリックします。
設定が完了すると通知されます。

ステップ 5 [ログインへ進む（Proceed to Login）] を選択します。

ステップ 6 amAdmin 用に、前に設定したユーザ名とパスワードを使用して展開した OpenAM Web アプリケーションにログインします。

ステップ 7 [アクセス コントロール（Access Control）] タブで、[/（最上位領域）（/（Top Level Realm））] をクリックします。

ステップ 8 [（Authentication認証）] タブで、[コア（Core）] をクリックします。

ステップ 9 [すべてのコアの設定（All Core Settings）] クリックします。

ステップ 10 [ユーザ プロファイル（User Profile）] を [無視（Ignored）] に設定します。

ステップ 11 プロファイルを更新するには、[保存（Save）] をクリックします。

ステップ 12 OpenAM GUI からログアウトします。

OpenAM サーバでのポリシーの設定

次の表で詳しく説明するポリシー ルールを使用して OpenAM サーバ ポリシーをセットアップします。

表 *22*：ポリシー ルール

サービス タイプ（Service Type）	Name	リソース名	操作
URL のポリシー エージェント（リソース名を含む）	<hostname>-01	`https://<IMP FQDN>/*`	Enable GET, Value = Allow Enable POST , Value = Allow
	<hostname>-02	`https://<IMP FQDN>/*?*`	
	<hostname>-03	`https://<IMP FQDN>/*?*?*`	
	<hostname>-04	`https://<IMP FQDN>:8443/*`	
	<hostname>-05	`https://<IMP FQDN>:8443/*?*`	
	<hostname>-06	`https://<IMP FQDN>:8443/*?*?*`	

この手順で定義されているとおりにポリシー ルールを適用すると、IM and Presence の管理/ユーザ インターフェースは次の URL 形式を使用して Web ブラウザでのみアクセスが可能になります。

- `https://<IMP FQDN>`：たとえば、`https://IMP-Node-01.cisco.com`
- `https://<IMP FQDN>:8443`：たとえば、`https://IMP-Node-01.cisco.com:8443/`

`https://<IMP HOSTNAME>`（たとえば、`https://IMP-Node-01/`）などのホスト名だけを指定する URL を使用して Cisco Unified CM IM and Presence の管理/ユーザ インターフェイスにアクセスすることはできません。

手順

ステップ 1 OpenAM 管理インターフェイスにログインします。

ステップ 2 [アクセス コントロール（Access Control）] タブで、[/（トップ レベルのレルム）（/（Top Level Realm））] を選択します。

ステップ 3 [ポリシー（Policies）] タブで、[新規ポリシー（New Policy）] をクリックします。

ステップ 4 [名前（Name）] フィールドに、ポリシー名（IMPPolicy など）を入力し、[OK（OK）] をクリックします。
IMPPolicy はあくまでも推奨値です。有効な名前の値を使用できます。この後の設定では、この値は必要ありません。

ステップ 5 編集のために、新しいポリシー [IMPPolicy（IMPPolicy）] を選択します。

ステップ 6 [ルール（Rules）] をクリックします。

ステップ 7 次の順序でルールを追加します。

a) [ルール（Rules）] セクションで、[新規（New）] をクリックします。
b) [URL のポリシー エージェント（リソース名を含む）（URL Policy Agent（with resource name））] として [サービス タイプ（Service Type）] を選択します。
c) [次へ（Next）] をクリックします。
d) [名前（Name）] フィールドでは、上記のポリシー ルール テーブルの推奨されたルールの名前を入力し、<hostname> を IM and Presence ノードの実際のホスト名で置き換えます。
e) 提供される [リソース名（ResourceName）] フィールドで IM and Presence ノードの実際の完全修飾ドメイン名と <IMP FQDN> に代わり、このルールに対応するリソース名を入力します。
f) Allow 値で Get アクションを確認します。
g) Allow 値で POST アクションを確認します。
h) ルールの更新を完了するには、[終了（Finish）] をクリックします。
i) ポリシー アップデートを保存するには、[保存（Save）] をクリックします。
j) 上記テーブルのルールごとにこの手順全体を繰り返し、[終了（Finish）] をクリックします。

SSO の有効な各 IM and Presence サービス ノードに、この 6 つのルールのセットを追加する必要があります。

ステップ 8 ポリシーに 1 つのサブジェクトを追加する必要があります。次のようにサブジェクトを追加します。

a) [サブジェクト（Subject）] セクションで、[新規（New）] をクリックします。
b) [サブジェクト（Subject）] タイプとして[認証ユーザ（Authenticated Users）] を選択します。
c) [次へ（Next）] をクリックします。
d) [名前（Name）] 値として「IMPSubject」を入力します。
IMPSubject はあくまでも推奨値です。任意の有効な値を使用できます。この後の設定で、この値は必要ありません。
e) サブジェクトの更新を完了するには、[終了（Finish）] をクリックします。
f) ポリシー アップデートを保存するには、[保存（Save）] をクリックします。

複数の IM and Presence サービス ノードがシングル サインオンで有効な場合は、1 つのサブジェクトだけがこのポリシーで必要です。

ステップ 9 ポリシーに 1 つの条件を追加する必要があります。次のように条件を追加します。

a) [条件（Conditions）] セクションで、[新規（New）] をクリックします。
b) 条件タイプとして [アクティブ セッション タイム（Active Session Time）] を選択します。
c) [次へ（Next）] をクリックします。
d) [名前（Name）] 値として「IMPTimeOutCondition」を入力します。
IMPTimeOutCondition はあくまでも推奨値です。有効な名前の値を使用できます。この後の設定で、この値が必要です。
e) [最大セッション時間（分）（Maximum Session Time（minutes））] として「120」を入力します。
f) [セッションの終了（Terminate Session）] フィールドが [いいえ（No）] に設定されていることを確認します。
g) サブジェクトの更新を完了するには、[終了（Finish）] をクリックします。
h) ポリシー アップデートを保存するには、[保存（Save）] をクリックします。

複数の IM and Presence サービス ノードが SSO で有効な場合は、1 つの条件だけがこのポリシーで必要であることに注意してください。

SSO モジュール インスタンスの設定

この単一のモジュール インスタンスは、同じ Active Directory ドメインが展開全体で使用されている限り、SSO が設定されている複数の IM and Presence サービス ノードを共有することができます。複数の Active Directory ドメインを含む導入シナリオでは、このマニュアルでは説明しません。

手順

ステップ 1 OpenAM 管理インターフェイスにログインします。

ステップ 2 [アクセス コントロール（Access Control）] タブから、[トップ レベルのレルム（Top Level Realm）] をクリックします。

ステップ 3 [認証（Authentication）] タブで、[モジュール インスタンス（Module Instances）] をクリックします。

ステップ 4 [モジュール インスタンス（Module Instances）] ウィンドウで、[新規（New）] をクリックします。

ステップ 5 新しいログイン モジュール インスタンス名（IMPKRBなど）を入力して、[タイプ（Type）] リストから [Windows デスクトップ SSO（Windows Desktop SSO）] を選択します。

ステップ 6 [OK] をクリックします。
このモジュール インスタンス名は、後で IM and Presence ノードで SSO を有効にするときに使用されます。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 [モジュール インスタンス（Module Instances）] ウィンドウで、新しいログイン モジュールの名前（たとえば、IMPKRB）を選択し、次の情報を入力します。

パラメータ	説明
Service Principal	この値はシングル サインオンの Active Directory をプロビジョニングするときに指定された値とまったく同じである必要があります。たとえば、- princ 値です。 たとえば、（openAM のサーバ名とドメインを使用して）`HTTP/server1.cisco.com@CISCO.COM`。
Keytab File Name	この値はシングル サインオンの Active Directory をプロビジョニングしたときに作成されたキータブ ファイルの場所である必要があります。 たとえば、（Windows プラットフォームで）`C:\keytab\server1.HTTP .keytab` です。

パラメータ	説明
Kerberos Realm	OpenAM サーバのドメイン。たとえば、`CISCO.COM`。
Kerberos Server Name (Active Directory)	AD サーバの FQDN を提供します。AD サーバは通常、Kerberos ドメイン コントローラです。フェールオーバーの目的で複数の Kerberos ドメイン コントローラが存在する場合は、区切り文字としてコロン（：）を使用してすべての Kerberos ドメイン コントローラを設定できます。たとえば、`ad.cisco.com` です。
Authentication Level	たとえば、22 です。

ステップ 9 [保存（Save）] をクリックします。
モジュール インスタンスが IMPKRB という名前で作成されます。

ステップ 10 SSO モジュールが有効な Windows ユーザとしてWindows デスクトップ セッションにログインすることで正常に機能することを確認します（AD に存在する有効なエンド ユーザでログインし、管理者アカウントは使用しないでください）。次の URL にアクセスしてください。

（注） ブラウザに SSO が設定されている必要があります。

`https://<openam-FQDN>:8443/<war-file-name>/UI/Login?module=<SSO_Module>`

ここで、

パラメータ	説明
<openam-FQDN>	OpenAM サーバの FQDN。
<war-file-name>	導入される OpenAM War ファイルの名前。たとえば、opensso。
<SSO_Module>	WindowsDesktopSSO モジュールの名前。

画面がログインに成功したことを通知します。

OpenAM サーバでの J2EE エージェント プロファイルの設定

J2EE エージェントは、SSO が有効な各 IM and Presence Service ノードでインスタンス化される内部コンポーネントです。J2EE エージェントごとに、OpenAM サーバで関連する J2EE エージェントプロファイルを設定する必要があります。したがって、J2EEエージェントプロファイルはSSOが有効なすべての IM and Presence Service ノードで必要です。複数のノードを SSO 用に設定する場合は、J2EE エージェント プロファイルを追加の各ノードに作成する必要があります。

次の表に、IM and Presence Service ノードに必要な J2EE プロファイル エージェントのパラメータを一覧表示します。

表 *23*：*J2EE* プロファイルのエージェント セットアップ パラメータの説明

パラメータ	説明
名前	J2EE Policy Agent の名前。たとえば、<*hostname-j2ee-agent*>。この場合、*hostname* は IM and Presence Service ノードのホスト名（たとえば、impNode01 j2ee agent）です。
Password	J2EE Policy Agent のパスワード。 （注） パスワードは IM and Presence Service で SSO を有効にするときに使用されます。
Configuration	J2EE Policy Agent 設定が保存されている場所を制御します。 [一元化（Centralized）] を選択します。
Server URL	OpenAM サーバの完全な URL。 たとえば、`https://<OpenAM FQDN>:8443/opensso`。この場合、`opensso` は .war 拡張子が削除された OpenAM War ファイルの名前です。
Agent URL	OpenAM が通知をパブリッシュする J2EE Policy Agent の URL。 たとえば、`https://<IMP FQDN>:8443/agentapp` （注） 値「`agentapp`」は上記のサンプル URL の重要項目です。`agentapp` 値を使用する場合、「ポリシー エージェントが展開される場所に関連するパスを入力してください」というプロンプトが表示されたときに「`agentapp`」と入力します。

次の表に、IM and Presence Service の各 Web GUI アプリケーションのログイン フォームの URI を一覧表示します。

表 *24*：*IM and Presence Service* の *Web GUI* アプリケーションの ログイン フォームの *URI*

Application	サンプル値
Cisco Unified CM IM and Presence の管理	`/cupadmin/WEB-INF/pages/logon.jsp`
Cisco Unified IM and Presence サービスアビリティ	`/ccmservice/WEB-INF/pages/logon.jsp`
Cisco Unified IM and Presence のレポート	`/cucreports/WEB-INF/pages/logon.jsp`
Cisco Unified IM and Presence OS の管理	`/cmplatform/WEB-INF/pages/logon.jsp`
IM and Presence のディザスタ リカバリ システム	`/drf/WEB-INF/pages/logon.jsp`

Application	サンプル値
Real Time Monitoring Tool（RTMT）	`/ast/WEB-INF/pages/logon.jsp`
Cisco Client Profile Agent	`/ssoservlet/WEB-INF/pages/logon.html`

手順

ステップ 1 OpenAM 管理インターフェイスにログインします。

ステップ 2 [アクセス コントロール（Access Control）] タブで、[/（最上位領域）（/（Top Level Realm））] をクリックします。

ステップ 3 [エージェント（Agents）] タブから、[J2EE（J2EE）] タブを選択します。

ステップ 4 [エージェント（Agents）] セクションで、[新規（New）] をクリックします。

ステップ 5 J2EE セットアップ パラメータを入力します。

ステップ 6 [作成（Create）] をクリックします。
<hostname-j2ee-agent> の名前で J2EE エージェントが作成されます。

ステップ 7 作成した J2EE エージェントを選択します。

ステップ 8 [ログイン処理（Login Processing）] セクションの下の [アプリケーション（Application）] タブで、IM and Presence Service の各 Web GUI アプリケーションの ログイン フォームの URI を追加します。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 [OpenAM サービス（OpenAM Services）] タブで、`https://<OpenAM FQDN>:8443/<war-file-name>/UI/Login?module=<SSO_Module>` のように OpenSSO のログイン URL を追加します。

ヒント 入力する *<SSO_Module>* 値が SSO モジュール インスタンスをセットアップするときに入力した値と一致する必要があります。たとえば、`https://server1.cisco.com:8443/opensso/UI/Login?module=IMPKRB` です。

ステップ 11 テキスト領域で、ログイン URL 以外のすべての URL を削除します。前のステップで指定したログイン URL のみがテキスト領域にリストされている必要があります。

ステップ 12 [保存（Save）] をクリックします。

ステップ 13 [メイン ページに戻る（Back to Main Page）] をクリックします。

ステップ 14 SSO 用に有効にするその他すべての IM and Presence Service ノードの J2EE プロファイル エージェントを作成するために、ステップ 4 から ステップ 13 を繰り返します。

関連トピック

GUI を使用した シングル サインオンの有効化, （191 ページ）

OpenAM セッション タイムアウトの設定

OpenAM セッション タイムアウトは、IM and Presence サービス ノードにセットされるセッション タイムアウト パラメータよりも大きい値に設定する必要があります。IM and Presence サービス ノードのセッション タイムアウト値を決定するには、CLI を使用して次のコマンドを入力してください。

show webapp session timeout

手順

ステップ 1 OpenAM 管理インターフェイスにログインします。

ステップ 2 [設定（Configuration）] タブで、[グローバル（Global）] を選択します。

ステップ 3 [セッション（Session）] をクリックします。

ステップ 4 [ダイナミック属性（Dynamic Attributes）] をクリックします。

ステップ 5 [最大アイドル時間（Maximum Idle Time）] フィールドに値を入力します。

ステップ 6 [保存（Save）] をクリックします。

IM and Presence サービスへの OpenAM 証明書のインポート

SSO の IM and Presence サービス ノードは、暗号化されたチャネル経由の OpenAM サーバと通信します。暗号化された通信チャネルの確立は、OpenAM サーバによって提示されるセキュリティ証明書を信頼するために、SSO を有する各 IM and Presence サービス ノードが必要です。IM and Presence サービス ノードは tomcat-trust の信頼ストアに必要なセキュリティ証明書をインポートすることで、セキュリティ証明書を信頼します。

必要な手順は、OpenAM サーバの Java キーストアの作成時に使用するセキュリティ設定によって異なります。

- OpenAM/Tomcat インスタンスの自己署名セキュリティ証明書を使用します。
- OpenAM/Tomcat インスタンスの CA 署名付きセキュリティ証明書を使用します。

注意 OpenAM 証明書のインポートはサービスに影響し、メンテナンス時間帯に OpenAM 証明書をインポートすることを強く推奨します。

（注） 証明書のインポートの詳細については、『*Cisco Unified System Maintenance Guide for IM and Presence*』を参照してください。

手順

ステップ 1 SSO 対応の IM and Presence データベース パブリッシャ ノードの Cisco Unified CM IM and Presence の管理にログインします。

ステップ 2 [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。

ステップ 3 証明書信頼ストアとして [Tomcat 信頼（Tomcat Trust）] を選択します。

ステップ 4 [ピア サーバ（Peer Server）] として OpenAM サーバの完全修飾ドメイン名を入力します。

ステップ 5 [ピア サーバ ポート（Peer Server Port）] として 8443 を入力します。

ステップ 6 [送信（Submit）] をクリックします。
証明書インポート ツールは 2 種類のテストを実行します。

- [指定した証明書サーバ（ping が可能）の到達可能性の確認（Verify reachability of the specified certificate server （pingable））] : OpenAM サーバが、この IM and Presence のノードに到達可能なことを確認します。このテストに失敗する場合は、ping 操作をブロックする OpenAM ベースの Windows システム ファイアウォールが原因である可能性があります。Windows ファイアウォールで ping を許可する IM and Presence サービスへの OpenAM 証明書のインポートに関連するトピックを参照してください。
- [指定した証明書サーバへの SSL 接続の確認（Verify SSL connectivity to the specified certificate server）] : この IM and Presence ノードが OpenAM サーバに安全に接続することが可能かどうかを確認します。このテストが「証明書の欠落」によって失敗する場合は、必要な証明書が見つからず、セキュアな接続を確立できません。このテストが失敗した場合は、次の手順に進みます。このテストに成功した場合、ステップ 15 に進みます。

  （注） このテストが「トラブルシュータで内部エラーが発生しました」のメッセージが表示されて失敗する場合、次のステップに進む前に、証明書の障害をトラブルシューティングします。

ステップ 7 [設定（Configure）] をクリックして証明書ビューアを開きます。証明書ビューアは、TLS 接続ハンドシェイク中に OpenAM から提示される証明書チェーンを視覚的に表示します。これは、この IM and Presence サービス ノードにインポートされる必要がある証明書を表示します。

ステップ 8 チェーンの証明書を検査し、発行者が信頼できることを確認します。

ステップ 9 [証明書チェーンを許可する（Accept Certificate Chain）] のチェックボックスをオンにし、[保存（Save）] をクリックします。
チェーンから必要な証明書が、この IM and Presence サービス ノードの tomcat-trust の信頼ストアに今すぐインポートされます。

ステップ 10 [閉じる（Close）] をクリックします。
証明書のインポート ツールは「証明書が検証に成功」と報告します。

ステップ 11 次の CLI コマンドを使用して、このノードのCisco Intercluster Sync Agent サービスを再起動します。**utils service restart Cisco Intercluster Sync Agent**

ステップ 12 次の CLI コマンドを使用して、このノードで Tomcat サービスを再起動します。 **utils service restart Cisco Tomcat**

ステップ 13 このクラスタの各 IM and Presence サービス サブスクライバ ノードのステップ 11 と 12 を繰り返します。

ステップ 14 このクラスタの各サブスクライバノードの証明書のインポートツールを使用して、セキュアな接続を確認します。

a) SSO が設定されている IM and Presence サービス サブスクライバ ノードの Cisco Unified CM IM and Presence の管理にログインします。
b) [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。
c) 証明書信頼ストアとして [Tomcat 信頼（Tomcat Trust）] を選択します。
d) [ピア サーバ（Peer Server）] として OpenAM サーバの FQDN を入力します。
e) [ピア サーバ ポート（Peer Server Port）] として 8443 を入力します。

ステップ 15 SSO が有効なすべての IM and Presence サービス クラスタのための、この手順を繰り返します。

関連トピック

シングル サインオンの設定前の重要な情報, （162 ページ）
証明書エラー, （281 ページ）

シングル サインオンのアクティブ化

SSO を有効にする場合は、ここに示す順序で次のタスクを実行する必要があります。

注意 SSO を有効にするとサービスに影響を与えます。そのため、メンテナンス時に、SSO を有効にすることを推奨します。

SSO 有効化前のアクセス権限の設定

SSO の有効化前および有効化後に設定されている必要があるユーザ アクセス権限を理解することが重要です。権限を理解することで、IM and Presence Service アプリケーションにアクセスするときにユーザの権限が誤っているという状況を避けることができます。

表 *25*：シングル サインオンを有効化するための前提条件

Application	注記

Cisco Unified CM IM and Presence の管理 • Cisco Unified CM IM and Presence の管理 • IM and Presence サービスアビリティ • IM and Presence のレポート	

SSO を有効にする前に、管理アクセスを容易にするために必要なユーザ グループのメンバーであるエンド ユーザが存在していることを確認します。

インストール時に作成されたデフォルトの管理者アプリケーション ユーザには次が必要です。

グループ：

- 標準監査ユーザ
- 標準 CCM スーパー ユーザ

権限：

- Standard AXL API Access
- 標準 Admin Rep Tool Admin
- 標準監査ログ管理
- Standard CCM Admin Users
- Standard CCMADMIN Administration
- 標準 CUReporting
- 標準 EM 認証プロキシ権
- Standard SERVICEABILITY Administration
- 標準 SSO 設定管理

これらの役割を持つ上記のユーザ グループのメンバーであるユーザには、デフォルトの管理者と同様に、IM and Presence Service への完全なアクセス権があります。

IM and Presence Service のデフォルトのアプリケーション ユーザを表示するには、[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [ユーザ管理（User Management）] > [アプリケーション ユーザ（Application User）] > [検索（Find）] を選択します。詳細を表示するには、デフォルトのアプリケーション ユーザ（インストール時に作成されたユーザ）を選択します。

IM and Presence Service のこれらのグループにエンド ユーザを追加するには、[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [アクセス制御グループ（Access Control Group）] > [検索（Find）] を選択します。グループを選択し、[エンド ユーザの追加（Add End Users）] をクリックします。目的のエンド ユーザを検索してそのユーザを選択し、[グループへのエンド ユーザの追加（Add End Users to Group）] をク

	リックします。
Cisco Unified IM およびプレゼンス オペレーティング システムの管理 • IM and Presence オペレーティング システムの管理 • IM and Presence のディザスタ リカバリ システム	通常、デフォルトの管理者アプリケーション ユーザはこれらの Web アプリケーションにアクセスできません。これらの Web アプリケーションには、Cisco Unified IM and Presence オペレーティング システムの管理者のみがアクセスできます。この管理者は、これらの Web アプリケーションに加え、管理 CLI にアクセスできます。 これらのアプリケーションに対して SSO が有効になった後は、デフォルトの管理者アプリケーション ユーザと同じ権限があるエンド ユーザがアプリケーションにアクセスできます。
Real-Time Monitoring Tool	SSO を有効にする前に、リアルタイム監視ツールへの管理アクセスを許可するために必要なユーザ グループのメンバーであるエンド ユーザが存在することを確認します。 上記の Cisco Unified CM IM and Presence の管理の注記を参照してください。

GUI を使用した シングル サインオンの有効化

この Cisco Unified IM and Presence オペレーティング システムの管理アプリケーションは、3 個のコンポーネントに分割されます。

- ステータス
- サーバの設定
- アプリケーションの選択

ステータス

SSO 設定の変更によって、Tomcat が再起動することを示す警告メッセージが表示されます。

SSO アプリケーションを有効にすると、次のエラー メッセージが表示されることがあります。

- 無効な Open Access Manager（OpenAM）サーバの URL（Invalid Open Access Manager (OpenAM) server URL）：無効な OpenAM サーバ URL を入力すると、このエラー メッセージが表示されます。
- 無効なプロファイル クレデンシャル（Invalid profile credentials）：間違ったプロファイル名または間違ったプロファイル パスワードあるいは両方を入力すると、このエラー メッセージが表示されます。
- セキュリティ信頼エラー：この IM and Presence サービス ノードが OpenAM server によって提示される証明書チェーンを信頼しない場合、このエラー メッセージが表示されます。

（注） SSO を有効にするときに上記のいずれかのエラーメッセージが表示された場合は、ステータスが該当するエラーに変更します。

サーバの設定

SSO がすべてのアプリケーションで無効になっている場合にのみ、サーバの設定を編集できます。

アプリケーションの選択

次のアプリケーションのいずれかを使用して SSO を有効または無効にできます。

- Cisco Unified CM IM and Presence の管理：Cisco Unified CM IM and Presence の管理、Cisco Unified IM and Presence のサービスアビリティ、および Cisco Unified IM and Presence のレポートに対して SSO を有効にします。
- 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 オペレーティング システムの管理およびディザスタ リカバリ システムに対して SSO を有効にします。
- RTMT： Real-Time Monitoring Tool 用に Web アプリケーションを有効にします。
- Cisco UP Client Profile Agent：Cisco UP Client Profile Agent サービスの SSO を有効にします。このオプションは、共通アクセスカード（Common Access Card）（CAC） Sign-On を使用する顧客にのみ適用されます。

手順

ステップ 1 [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 Operating SystemAdministration）] > [セキュリティー（Security）] > [シングル サインオン（Single Sign On）] を選択します。

ステップ 2 Open Access Manager（OpenAM）サーバの URL を入力します。

例：

`https://server1.cisco.com:8443/opensso`

ステップ 3 ポリシー エージェントを展開する相対パスを入力します。相対パスは、英数字（*agentapp* など）にする必要があります。

ステップ 4 このポリシーエージェント用に設定されたプロファイルの名前（たとえば「cupnode01 j2ee エージェント」）を入力します。

ステップ 5 プロファイル名のパスワードを入力します。

ステップ 6 「IMPKRB」などの、Windows デスクトップ SSO 用に設定されたログイン モジュール インスタンス名を入力します。詳細については、SSO のモジュール例のセットアップに関するトピックを参照してください。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 [確認（Confirmation）] ダイアログボックスで、[OK（OK）] をクリックして Tomcat を再起動します。

シングル サインオンの非アクティブ化

SSO を無効にするには、ここに示す順序で次のタスクを実行します。

SSO 無効化前のアクセス権限の設定

SSO が SSO をサポートする任意のIM and Availability Web アプリケーションに対して無効になっている場合は、そのアプリケーションにアクセスするすべてのユーザにユーザ名とパスワードを提供する必要があります。IM and Presence Service 管理者が IM and Availability Web アプリケーションに対して SSO を無効にする場合は、SSO の無効化後にユーザがアプリケーションにアクセスできることを確認します。この操作は、アクティブな IM and Presence Service 管理アカウントを誤ってロック アウトしないようにするために重要です。

表 *26*：シングル サインオン無効化の前提条件

Application	注記

Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence の管理、IM and Presence のサービスアビリティ、IM and Presence のレポート）	SSO を無効にする前に、既知のユーザ名およびパスワードを持つアプリケーション ユーザが存在し、このユーザが必要なユーザ グループのメンバーであることを確認します。 インストール時に作成されたデフォルトの管理者アプリケーション ユーザには次が必要です。 グループ： • 標準監査ユーザ • 標準 CCM スーパー ユーザ 権限： • Standard AXL API Access • 標準 Admin Rep Tool Admin • 標準監査ログ管理 • Standard CCM Admin Users • Standard CCMADMIN Administration • 標準 CUReporting • 標準 EM 認証プロキシ権 • Standard SERVICEABILITY Administration • 標準 SSO 設定管理 SSO が無効になっている場合は、これらの役割を持つ上記のユーザ グループのメンバーであるアプリケーション ユーザは IM and Presence Service に対する完全なアクセス権限を持つことになります。 IM and Presence のアプリケーション ユーザを表示するには、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [ユーザ管理（User Management）] > [アプリケーション ユーザ（Application User）] > [検索（Find）] を選択します。ユーザを選択して詳細を表示します。
Cisco Unified IM and Presence オペレーティング システムの管理（IM and Presence オペレーティング システムの管理、 IM and Presence DRS）	SSO を無効にする前に、既知のユーザ名およびパスワードを持つ OS 管理ユーザが存在し、このユーザに Cisco Unified IM and Presence オペレーティングシステム管理 CLI へのアクセス権があることを確認します。SSO を無効にした後に、このユーザには Cisco Unified IM and Presence オペレーティング システム管理 GUI へのアクセス権があります。

Real-Time Monitoring Tool	SSO を無効にする前に、既知のユーザ名およびパスワードを持つアプリケーション ユーザが存在しており、このユーザに Cisco Unified CM IM and Presence 管理（Cisco Unified CM IM and Presence の管理、IM and Presence のサービスアビリティ、および IM and Presence のレポート）に指定されたユーザと同じアクセス権があることを確認します。

シングル サイン オンの無効化

この手順で説明されているように、GUI または CLI を使用して SSO を無効にできます。CLI を使用して SSO を無効にする方法の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』の utils sso disable コマンドを参照してください。

手順

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] > [セキュリティ（Security）] > [シングル サインオン（Single Sign On）] を選択します。

ステップ 2 前に SSO 用に有効にしたすべてのアプリケーションを選択解除します。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 [確認（Confirmation）] ダイアログボックスで、[OK（OK）] をクリックして Tomcat を再起動します。

Windows での OpenAM のアンインストール

はじめる前に

OpenAM をアンインストールする前に、次の作業が完了していることを確認します。

- SSO を無効にする前に、アクセス権限を設定します。
- シングル サイン オンの無効化

手順

ステップ 1 OpenAM サーバの Windows デスクトップにアクセスし、[開始（Start）] > [すべてのプログラム（All Program）] > [Apache Tomcat 7.0 Tomcat7] > [Tomcat の設定（Configure Tomcat）] を選択します。

（注） このメニュー パスは Tomcat 7. を使用していることを前提としています。

ステップ 2 OpenAM サーバ上で Tomcat サービスが動作している場合は、[全般（General）] タブで [停止（Stop）] をクリックし、サービスを停止します。

ステップ 3 OpenAM 設定データを削除します。このデータは通常、Tomcat インスタンスを実行しているユーザのホームディレクトリにある 2 つのディレクトリに保存されています。たとえば、`C:\opensso`（フォルダ名が、`opensso` などの OpenAM WAR ファイルの展開済みの URI と一致する場合）や、`C:\.openssocfg` などです。

ステップ 4 OpenAM/Tomcat インスタンスの `tomcat-dir\webapps` から、展開済みの OpenAM WAR ファイルと WAR ファイル自体を削除します。

例：
`C:\Program Files\Apache Software Foundation\Tomcat 7\webapps`

ヒント Tomcat ディレクトリ変数の説明については、Tomcat のインストールに関するトピックを参照してください。

ステップ 5 OpenAM サーバの Windows デスクトップにアクセスし、[開始（Start）] > [すべてのプログラム（All Program）] > [Apache Tomcat 7.0 Tomcat7] > [Tomcat の設定（Configure Tomcat）] を選択します。

ステップ 6 [全般（General）] タブで、[開始（Start）] をクリックして Tomcat サービスを起動します。

関連トピック

SSO 無効化前のアクセス権限の設定, （193 ページ）
シングル サイン オンの無効化, （195 ページ）
Tomcat のインストール, （173 ページ）

デバッグ レベルの設定

J2EE Policy Agent のログ レベルの設定に従い、IM and Presence サービス ノードの追加デバッグ情報を収集できます。このコンポーネントのログ レベルは OpenAM サーバで設定されます。デフォルトのログ レベルはエラーです。追加デバッグ情報を提供するためにログ レベルをメッセージ（Message）に変更できます。関連ログ ファイルが非常に大きくなる場合があるので、短期間だけメッセージ ログ レベルを使用することを推奨します。

手順

ステップ 1 Web ブラウザ（たとえば、Mozilla Firefox）から OpenAM（`https://<OpenAM FQDN>:8443/opensso`）にサインインします。

ステップ 2 [アクセス コントロール（Access Control）] メニューから、[トップ レベルのレルム（Top Level Realm）] > [エージェント（Agents）] > [J2EE] を選択します。

ステップ 3 [全般（General）] 見出しの下で、[エージェントのデバッグ レベル（Agent Debug Level）] を選択します。

ステップ 4 [エージェントのデバッグ レベル（Agent Debug Level）] を下で、目的のレベルを指定します（メッセージまたはエラー）。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 IM and Presence サービス ノードで Cisco Tomcat サービスを再起動します。

a) IM and Presence の管理 CLI にアクセスします。

b) 次のコマンドを実行します。**utils service restart Cisco Tomcat**

ステップ 7 SSO コンポーネントのログを参照およびダウンロードしてから、IM and Presence サービスのCisco Unified Real Time Monitoring Tool を使用してログを取得します。

（注） SSO が有効になっているときに問題が発生する場合は、SSO を無効にして、Cisco Unified Real Time Monitoring Tool から debug.out logs にアクセスするために SSO を再び有効にする必要があります。

第 IV 部

管理（Administration）

第 13 章

チャットの設定と管理

チャット展開

異なる展開シナリオに合わせてチャットを設定できます。展開シナリオの例を使用できます。

チャットの展開シナリオ 1

展開シナリオ：	チャット ノードのエイリアスにクラスタ ID を含めません。システムで生成されたエイリアス `conference-1-mycup.cisco.com` ではなく、エイリアス `primary-conf-server.cisco.com` を使用します。
設定手順：	**1** [Messaging（メッセージング）] > [Group Chat and Persistent Chat（グループ チャットとパーシステント チャット）] を選択して、システムで生成されたエイリアスをオフにします（これはデフォルトでオンになっています）。 **2** エイリアスを編集し、`primary-conf-server.cisco.com`に変更します。
（注）	システムで生成された古いエイリアスをオフにすると、`conference-1-mycup.cisco.com` は、[グループ チャット サーバのエイリアス （Group Chat Server Alias）] の下に表示される標準の編集可能なエイリアスに戻ります。これにより、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 ルームのアドレスが維持されます。

チャットの展開シナリオ 2

展開シナリオ：	目的： • ドメインを cisco.com から linksys.com に変更し、conference-1-mycup.cisco.com ではなく、conference-1-mycup.linksys.com を使用します。 • ユーザがまだ xxx@conference-1-mycup.cisco.com というタイプの古いチャット ルームを検索できるように、データベース内の既存の永続的なチャット ルームのアドレスを維持します。
設定手順：	1 **Cisco Unified CM IM and Presence Administration** にログインして、[プレゼンス（Presence）]>[トポロジの設定（Settings Topology）]> [詳細設定（Advanced Configuration）] を選択します。 2 デフォルトの IM and Presence Service ドメインの編集方法の詳細については、関連するトピックを参照してください。
（注）	ドメインを変更すると、完全修飾クラスタ名（FQDN）が conference-1-mycup.cisco.com から conference-1-mycup.linksys.com に自動的に変更されます。システムで生成された古いエイリアス conference-1-mycup.cisco.com は、[グループ チャット サーバのエイリアス（Group Chat Server Aliases）] の下に表示される標準の編集可能なエイリアスに戻ります。これにより、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が維持されます。

関連トピック

IM and Presence Service のデフォルトのドメイン設定

チャットの展開シナリオ 3

展開シナリオ：	目的： • mycup から ireland にクラスタ ID を変更し、conference-1-mycup.cisco.com ではなく、conference-1-ireland.cisco.com を使用します。 • データベース内の既存の永続的なチャットルームのアドレスを維持する必要はありません。
設定手順：	1 [Cisco Unified CM IM and Presence の管理 （Cisco Unified CM IM and Presence Administration）]>[プレゼンス（Presence）]>[設定（Settings）]>[標準設定（Standard Configuration）] を選択します。

	2 クラスタ ID を編集し、ireland に変更します。 **3** [メッセージング（Messaging）] > [グループ チャット サーバ エイリアスのマッピング（Group Chat Server Alias Mapping）] を選択します。 **4** 古いエイリアス conference-1-mycup.cisco.com を削除します。
（注）	クラスタ ID を変更すると、完全修飾クラスタ名（FQDN）が conference-1-mycup.cisco.com から conference-1-ireland.cisco.com に自動的に変更されます。システムで生成された古いエイリアス conference-1-mycup.cisco.com は、[グループ チャット サーバ エイリアス（Group Chat Server Aliases）] の下に表示される標準の編集可能なエイリアスに戻ります。これにより、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 ルームのアドレスが維持されます。（この例では）管理者は古いエイリアス アドレスを維持する必要がないため、これを削除するのが適切です。

チャットの展開シナリオ 4

展開シナリオ：	目的： • 既存のエイリアスに関連付けられたノード（たとえば、conference-3-mycup.cisco.com）をシステム トポロジから削除します。 • 新しいノード ID（ノード ID：7）を持つ新しいノード（たとえば、conference-7-mycup.cisco.com）をシステム トポロジに追加します。 • 古いエイリアスを使用して作成されたチャット ルームのアドレスを維持します。
設定手順：	オプション 1 **1** [Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] > [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）] を選択します。 **2** [新規追加（Add New）] を選択して、追加エイリアス conference-3-mycup.cisco.com を追加します。 オプション 2 **1** [メッセージング（Messaging）] > [グループ チャットおよび永続的なチャット（Group Chat and Persistent Chat）] を選択し、システムで生成されたデフォルト エイリアス conference-7-mycup.cisco.com をオフにします（これはデフォルトでオンになっています）。 **2** エイリアスを編集し、conference-3-mycup.cisco.com に変更します。

（注）	システム トポロジに新しいノードを追加すると、システムはノードに自動的にこのエイリアス（conference-7-mycup.cisco.com）を割り当てます。 オプション 1 • 追加エイリアスを追加すると、ノードは両方のエイリアス（conference-7-mycup.cisco.com と conference-3-mycup.cisco.com）によってアドレス指定可能です。 オプション 2 • システムで生成された古いエイリアスをオフにすると、conference-7-mycup.cisco.com は、[グループ チャット サーバのエイリアス（Group Chat Server Alias）] の下に表示される標準の編集可能なエイリアスに戻ります。

チャット管理の設定

IM ゲートウェイ設定の変更

IM and Presence サービスの IM ゲートウェイを設定できます。

IM and Presence サービスのIM Gateway のSIP ツー XMPP 接続（SIP-to-XMPP connection）はデフォルトで有効です。SIP と XMPP クライアント間の IM の相互運用性を実現することで、SIP IM クライアントのユーザが XMPP IM クライアントのユーザと二方向 IM を交換できるようになります。IM ゲートウェイ ステータス パラメータをオンにしておくことを推奨します。ただし、XMPP と SIP クライアントの相互通信を防ぐために、IM ゲートウェイ ステータス パラメータをオフにすることもできます。

IM 会話のデフォルトの非アクティブ タイムアウト間隔も変更でき、IM が送信に失敗した場合に表示されるエラー メッセージも選択できます。

制約事項

SIP クライアントは、XMPP 固有の機能であるチャット ルームに参加できません。

手順

ステップ 1 [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）] を選択します。

ステップ 2 **[サーバ（Server）]** 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。

ステップ 3 **[サービス パラメータ設定（Service Parameter Configuration）]** ウィンドウでサービスとして [Cisco SIP プロキシ（Cisco SIP Proxy）] を選択します。

ステップ 4 次のいずれか 1 つの処理を実行します。

a) この機能を有効にするために、[SIP XMPP IM ゲートウェイ（クラスタ全体）（SIP XMPP IM Gateway（Clusterwide））] セクションの [IM ゲートウェイ ステータス（IM Gateway Status）] を [オン（ON）] に設定します。
b) この機能を無効にするために、[SIP XMPP IM ゲートウェイ（クラスタ全体）（SIP XMPP IM Gateway（Clusterwide））] セクションの [IM ゲートウェイ ステータス（IM Gateway Status）] を [オフ（Off）] に設定します。

ステップ 5 ゲートウェイによって維持される IM 会話の非アクティブなタイムアウト間隔（秒単位）を設定します。ほとんどの環境に適したデフォルト設定は 600 秒です。

ステップ 6 IM が配信に失敗した場合に、ユーザに表示するエラー メッセージを指定します。デフォルト エラー メッセージ：「Your IM could not be delivered（IM を配信できませんでした）」

ステップ 7 [保存（Save）] をクリックします。

次の作業

永続的なチャット ルームの設定に進みます。

ファイル転送の有効化

管理者は、ファイル転送機能（XEP-0096）の IM and Presence サービス ノードのサポートを有効または無効にできます。ファイル転送のサポートを有効にすると、XMPP クライアントはエンドユーザにファイル転送機能を拡張できます。

（注） ローカル ユーザとクラスタ間ピアの連絡先の間のファイル転送は、両方のクラスタで機能が有効になっている場合のみ可能です。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。

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

ステップ 3 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、Cisco XCP Router をサービスとして選択します。

ステップ 4 [ファイル転送を有効にする（Enable file transfer）] ドロップダウン リストから、[オン（On）] または [オフ（Off）] を選択します。

ステップ 5 [保存（Save）]をクリックします。

ステップ 6 クラスタ内の各ノードで Cisco XCP Router サービスを再起動します。

関連トピック

Cisco XCP ルータ サービスの再起動, （68 ページ）

サインイン セッション数の制限

管理者は Cisco XCP Router のユーザごとのサインイン セッションの数を制限できます。このパラメータは、XMPP クライアントのみに適用されます。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。

ステップ 2 [サーバ（Server）] 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。

ステップ 3 [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウでサービスとして [Cisco XCP ルータ（Cisco XCP Router）] を選択します。

ステップ 4 [XCP Manager 設定パラメータ（クラスタ全体）（XCP Manager Configuration Parameters（Clusterwide））] 領域の [ユーザごとのログオン セッションの最大数（Maximum number of logon sessions per user）] にパラメータ値を入力します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 Cisco XCP Router サービスを再起動します。

関連トピック

Cisco XCP ルータ サービスの再起動, （68 ページ）

永続的なチャット ルームの設定

一時的な（アドホック）チャットルームではなく永続的なチャットルームを使用する場合にのみ永続的なチャットの設定を行う必要があります。この設定は、永続的なチャットに固有で、法規制の遵守のための IM アーカイブに影響しません。

制約事項

SIP クライアントは、XMPP 固有の機能であるチャット ルームに参加できません。

はじめる前に

- 永続的なチャット ルームを使用するには、ノードごと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。
- 永続的なチャットのロギングに外部データベースを使用する場合は、データベースのサイズを考慮します。チャット ルームのすべてのメッセージをアーカイブすることはオプションで、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ます。大規

模な展開では、ディスク領域はただちに消費される可能性があります。データベースを、情報の量を処理するのに十分な大きさにしてください。

- 外部データベースへの接続数を設定する前に、オフラインで書き込む 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できます。
- 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。Cisco 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。

手順

ステップ 1 [Cisco Unified Communications Manager Cisco Unified CM IM and Presence の管理（Cisco IM and Presence Administration）] > [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）] を選択します。

ステップ 2 [パーシステントチャットの有効化（Enable Persistent Chat）] をオンにします。

（注） これはクラスタ全体の設定です。クラスタ内の任意のノードで永続的なチャットが有効になっている場合は、任意のクラスタのクライアントで、そのノード上の Text Conference インスタンスおよび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ルームを検出できます。

ステップ 3 （任意） チャット ルーム メッセージの保存方法を必要に応じて指定します。

a) ルームに送信されたすべてのメッセージをアーカイブする場合は、[すべてのルーム メッセージのアーカイブ（Archive all room messages）] をオンにします。これはすべての永続的なチャット ルームに適用されるクラスタ全体の設定です。

b) 要求を処理するために使用するデータベースへの接続の数を入力します。これは、チャット ノードと関連するデータベース間のすべての接続に適用されるクラスタ全体の設定です。

c) データベース接続を何秒後に更新するかを入力します。これは、チャット ノードと関連するデータベース間のすべての接続に適用されるクラスタ全体の設定です。

ステップ 4 事前設定された外部データベースのリストから選択し、チャット ノードに適切なデータベースを割り当てます。

ヒント [クラスタ トポロジの詳細（Cluster Topology Details）] ウィンドウでチャット ノードの詳細を編集する必要がある場合は、ハイパーリンクをクリックします。

ステップ 5 永続的なチャット設定を更新する場合、Cisco XCP Text Conference Manager サービスを再起動するために [Cisco Unified IM and Presence 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）] を選択します。

- [ルーム内のすべてのメッセージをアーカイブ（Archive all messages in a room）] 設定をオンにする場合は、永続的なチャットに使用する各外部データベースのパフォーマンスをモニタ

することを推奨します。データベースサーバで負荷が高くなることを予測する必要があります。

- 永続的なチャットルームを有効にし、外部データベースとの適切な接続を確立しない場合、TC サービスはシャットダウンします。このような状況では、すべてのチャットルームの機能（一時的および永続的の両方）が失われます。チャットノードが接続を確立すると（他のチャットノードが失敗しても）、そのノードは起動します。

次の作業

[Cisco XCP テキスト会議マネージャ（Cisco XCP Text Conference Manager）] をオンに設定します。

関連トピック

IM ゲートウェイ設定の変更, （204 ページ）
チャットノードエイリアスの管理, （212 ページ）

永続的なチャットの有効化

一時的な（アドホック）チャットルームではなく永続的なチャットルームを使用する場合にのみ、常設（パーシステント）チャットの設定を行います。この設定は、永続的なチャットに固有で、法規制の遵守のための IM アーカイブに影響しません。

はじめる前に

- 永続的な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。

重要 各ノードに外部データベースを割り当てておく必要があります。

- 永続的なチャットのロギングに外部データベースを使用する場合は、データベースのサイズを考慮します。チャットルームのすべてのメッセージをアーカイブすることはオプションで、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ます。大規模な展開では、ディスク領域はただちに消費される可能性があります。データベースを、情報の量を処理するのに十分な大きさにしてください。
- ルームの入退室をすべてアーカイブすると、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。
- 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できます。

- 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。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。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [メッセージング（Messaging）] > [グループ チャットと永続的なチャット（Group Chat and Persistent Chat）] を選択します。

ステップ 2 [パーシステントチャットの有効化（Enable Persistent Chat）] チェック ボックスをオンにします。

ステップ 3 （任意） ルームに入退室するユーザのすべてのインスタンスをログに記録するには、[すべてのルームの参加および終了をアーカイブ（Archive all room joins and exits）] チェック ボックスをオンにします。これはすべての永続的なチャット ルームに適用されるクラスタ全体の設定です。

ステップ 4 （任意） ルームに送信されたすべてのメッセージをアーカイブするには、[すべてのルームメッセージのアーカイブ（Archive all room messages）] チェック ボックスをオンにします。これはすべての永続的なチャット ルームに適用されるクラスタ全体の設定です。

ステップ 5 （任意） グループ チャット システム管理者だけが常設（永続的）チャット ルームを作成できるようにするには、[グループチャットのシステム管理者のみのパーシステントチャットルームの作成を許可する（Allow only group chat system administrators to create persistent chat rooms）] チェック ボックスをオンにします。これはすべての永続的なチャット ルームに適用されるクラスタ全体の設定です。
グループ チャット システムの管理者を設定するには、[メッセージング（Messaging）] > [グループ チャット システム管理者（Group chat system administrators）] を選択します。

ステップ 6 永続的なチャットルームの許容最大数を [許可された永続的なチャットルームの最大数（Maximum number of persistent chat rooms allowed）] フィールドに入力します。デフォルト値は 1500 に設定されています。

重要 外部データベースに十分な容量があることを確認する必要があります。多くのチャットルームを所有すると、外部データベースのリソースに影響を及ぼします。

ステップ 7 要求の処理に使用するデータベースへの接続数を [データベースへの接続数（Number of connections to the database）] フィールドに入力します。デフォルトでは 5 に設定されています。これは、チャット ノードと関連するデータベース間のすべての接続に適用されるクラスタ全体の設定です。

ステップ 8 データベース接続を更新するまでの秒数を [データベース接続ハートビート間隔（秒）（Database connection heartbeat interval (seconds)）] フィールドに入力します。デフォルトでは 300 に設定されています。これは、チャット ノードと関連するデータベース間のすべての接続に適用されるクラスタ全体の設定です。

ステップ 9 チャット ルームをタイムアウトにするまでの分数を [永続的なチャット ルームのタイムアウト値（分）（Timeout value for persistent chat rooms (minutes)）] フィールドに入力します。デフォルトでは 0 に設定されています。タイムアウトを使用して、チャット ルームがアイドルか空かを確認します。ルームがアイドルまたは空であると判明した場合は、そのルームは閉じられます。デフォルト値が 0 に設定されている場合は、アイドル チェックが無効になります。

ステップ 10 事前設定された外部データベースのリストから選択し、チャット ノードに適切なデータベースを割り当てます。

- [ルームのすべての入退室をアーカイブ（Archive all room joins and exits）] 設定をオンにした場合は、永続的なチャットルームに使用されている各外部データベースのパフォーマンスを監視することを推奨します。データベース サーバの負荷が高くなると考えられます。
- [すべてのルーム メッセージをアーカイブ（Archive all room messages）] 設定をオンにした場合は、永続的なチャットルームに使用されている各外部データベースのパフォーマンスを監視することを推奨します。データベース サーバの負荷が高くなると考えられます。
- 永続的なチャットルームを有効にし、外部データベースとの適切な接続を確立しない場合、チャット ノードは失敗します。このような状況では、すべてのチャット ルームの機能（一時的および永続的の両方）が失われます。チャットノードが接続を確立すると（他のチャット ノードが失敗しても）、そのノードは起動します。
- [クラスタ トポロジの詳細（Cluster Topology Details）] ウィンドウで Cisco Unified Communications Manager の IM and Presence Service ノードの詳細を編集するには、ハイパーリンクをクリックします。

ステップ 11 [保存（Save）] をクリックします。

ステップ 12 [Cisco Unified CM 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 - ネットワーク サービス（Control Center - Network Services）] を選択して、クラスタ内のすべてのノードの Cisco XCP Router を再起動します。
次の点に注意してください。

- Cisco XCP Text Conference Manager サービスがすでに実行されていた場合は、Cisco XCP Router を再起動すると、それも自動的に再起動します。
- Cisco XCP Text Conference Manager サービスがまだ実行されていなかった場合は、Cisco XCP Router が再起動した後にそれを手動で開始する必要があります。Cisco XCP Text Conference Manager サービスを開始するには、[Cisco Unified CM 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 - 機能サービス（Control Center - Feature Services）] を選択します。

（注） 永続的なチャットを有効にした後で、引き続き永続的なチャットの設定を更新する場合は、次の非動的設定にのみ、Cisco XCP Text Conference Manager の再起動が必要になります。

- 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）

関連トピック

Cisco XCP Text Conference Manager サービスの再起動

グループ チャット システム管理の設定

手順

ステップ 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。

ステップ 2 [グループ チャット システムの管理者を有効にする（Enable Group Chat System Administrators）] のチェックボックスをオンにします。
設定が有効または無効の場合、Cisco XCP ルータ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。

ステップ 3 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 5 ニックネームを入力します。

ステップ 6 説明を入力します。

ステップ 7 [保存（Save）] をクリックします。

グループ チャットと永続的なチャットのデフォルト設定と復帰

強化されたデフォルトのアドホックと永続的なチャットの設定を変更できます。すべての設定をデフォルト値に戻すには、[デフォルトに設定（Set to Default）] をクリックします。

（注） チャット ルームの所有者が設定を変更できるようにするには、ノードで [ルーム所有者が変更できる（Room owners can change）] チェック ボックスを選択します。ルームの所有者は、希望する設定や、作成しているルームに適用可能な設定を行えるようになります。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。

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

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。

（注） このチャット ノードのエイリアス（たとえば、conference-3-mycup.cisco.com）は、そのノードで作成された各チャット ルームの一意の ID 部分になります（roomjid@conference-3-mycup.cisco.com）。

次の方法で、クラスタ全体にエイリアスを割り当てることができます。

- システム生成：システムは一意のエイリアスを各チャット ノードに自動的に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を有効にする場合、チャット ノードに対処するためにさらに実行することはありません。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 ノードごとに 1 個のエイリアスを自動生成します。
  - conference：ハードコードされたキーワード
  - x：ノード ID を示す一意の整数値
  - 例：conference-3-mycup.cisco.com
- 手動：conference-x-clusterid.domain の命名規則が適さない場合、たとえば、チャット ノードのエイリアスにクラスタ ID を含めない場合は、システムで生成されたデフォルトのエイリアスを上書きすることもできます。手動管理されたエイリアスにより、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完全な柔軟性が得られます。
- 追加エイリアス：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。これは、システムによって生成されるエイリアスを割り当てるか、またはエイリアスを手動で管理するかに関係なく適用されます。

重要な考慮事項

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（System）] > [プレゼンス トポロジの設定（Presence Topology Settings）] 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（Presence）] > [プレゼンスの設定（Presence Settings）] 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て、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。

関連トピック

チャットの展開シナリオ 1, （201 ページ）

システムで生成されたチャット ノード エイリアスのオン/オフの切り替え

チャット ノード エイリアスを使用すると、任意のドメイン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、それらのチャット ルームに入室できます。デフォルトでは、IM and Presence Service によって、各ノードにシステムで生成された一意のエイリアスが自動的に割り当てられます。システムで生成されたエイリアスを使用する場合は、チャット ノードに対応するための設定はこれ以上必要ありません。システムは、デフォルトの命名規則である `conference-x-clusterid.domain` を使用して、チャット ノードごとに 1 個のエイリアスを自動的に生成します。

手動でチャット ノードエイリアスを割り当てる場合は、システムで生成されたデフォルトのエイリアス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 エイリアスの下にリストされる標準的な編集可能エイリアスに戻ります。詳細については、手動管理のチャット ノード

エイリアスに関するトピックを参照してください。ベスト プラクティスのガイドラインについては、サンプルのチャット展開シナリオを参照してください。

はじめる前に

- チャット ノード エイリアスと重要な考慮事項に関するトピックを参照してください。
- システムで生成されたエイリアス（`conference-3-mycup.cisco.com` など）は編集または削除できません。

手順

ステップ 1 **[Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）]** にログインし、[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）] を選択します。

ステップ 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。

a) システムでルーム チャット エイリアスを命名規則 `conference-x-clusterid.domain` を使用してノードに自動的に割り当てるようにするには、[システムでプライマリ グループ チャット サーバのエイリアスを自動的に管理する（System Automatically Manages Primary Group Chat Server Aliases）] チェックボックスをオンにします。

ヒント [メッセージング（Messaging）] > [グループ チャット サーバのエイリアス マッピング（Group Chat Server Alias Mapping）] を選択して、システムで生成されたエイリアスが [プライマリ グループ サーバのエイリアス（Primary Group Chat Server Aliases）] の下にリストされていることを確認します。

b) システムで生成されたエイリアスを無効にするには、[システムでプライマリ グループ チャット サーバのエイリアスを自動的に管理する（System Automatically Manages Primary Group Chat Server Aliases）] チェックボックスをオフにします。

次の作業

- 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ら、これらの操作のいずれかを実行します。
- Cisco XCP Text Conference Manager を再起動します。[Cisco Unified IM and Presence の有用性（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。

関連トピック

チャットの展開シナリオ 1, （201 ページ）
永続的なチャット ルームの設定, （206 ページ）

チャット ノードのエイリアスの手動管理

手動でチャット ノードのエイリアスを追加、編集、または削除できます。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。これにより、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 ルームのアドレスが維持されます。

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の管理（Cisco Unified CM IM and Presence Administration）]** で [プレゼンスの設定（Presence Settings）] > [詳細設定（Advanced Settings）] を選択します。

はじめる前に

チャット ノードのエイリアスと重要な考慮事項に関するトピックを参照してください。

手順

ステップ 1 **[Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）]** にログインし、[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）] を選択します。

ステップ 2 [System Automatically Manages Primary Group チャット サーバ エイリアス（System Automatically Manages Primary Group Chat Server Aliases）] をオフにします。

ステップ 3 すべての既存のチャット ノードのエイリアスはグループ チャット サーバのエイリアスの下に一覧表示されます。エイリアス リストを表示するには、次の操作を実行します。

a) [メッセージング（Messaging）] > [グループ チャット サーバ エイリアスのマッピング（Group Chat Server Alias Mapping）] を選択します。

b) [検索（Find）] をクリックします。

ステップ 4 必要に応じて、次の 1 つまたは複数の操作を実行します。

既存のエイリアス（古いシステム生成またはユーザ定義のエイリアス）を編集します

a) 編集する既存のエイリアスのハイパーリンクをクリックします。

b) [グループ チャットサーバのエイリアス（Group Chat Server Alias）] フィールドでノードのエイリアスを編集します。ノードのエイリアスが一意であることを確認します。

c) この変更されたエイリアスを割り当てる適切なノードを選択します。

新しいチャット ノードのエイリアスを追加します

a) [新規追加（Add New）] をクリックします。

b) [グループ チャットサーバのエイリアス（Group Chat Server Alias）] フィールドにノードの一意のエイリアスを入力します。

c) 新しいエイリアスを割り当てる適切なノードを選択します。

既存のエイリアスを削除します

a) 削除するエイリアスのチェックボックスをオンにします。

b) [選択項目の削除（Delete Selected）] をクリックします。

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。

次の作業

- Cisco XCP Text Conference Manager をオンにします。

関連トピック

チャット展開, （201 ページ）

Cisco XCP Text Conference Manager のオン

この手順は、永続的なチャット ルームの設定を行うか、チャット ノードに手動で 1 つまたは複数のエイリアスを追加した場合に適用されます。また、ノードでアドホック チャットを有効にする場合もこのサービスをオンにする必要があります。

はじめる前に

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。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。

手順

ステップ 1 **Cisco 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 - 機能サービス（Control Center - Feature Services）] を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストからノードを選択し、[移動（Go）] をクリックします。

ステップ 3 [IM and Presence Service] セクションの [Cisco XCP Text Conference Manager サービス（Cisco XCP Text Conference Manager service）] の横にあるオプション ボタンをクリックしてサービスをオンにするか、[再起動（Restart）] をクリックしてサービスを再起動します。

ステップ 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。

ステップ 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。

関連トピック

永続的なチャット ルームの設定, （206 ページ）

チャット ルーム管理

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をサポートし、拡張できます。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

ステップ 1 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 16500 に設定されています。

ステップ 2 [保存（Save）] をクリックします。

メンバーの設定

メンバー設定では、チャットルームのメンバーシップをシステム レベルで制御できます。このような制御は、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ユーザの役に立ちます。必要に応じてメンバーを設定します。

手順

ステップ 1 デフォルトでメンバー専用ルームとしてルームを作成する場合は、[デフォルトでルームはメンバー専用です（Rooms are for members only by default）] 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、そのルームの所有者または管理者が設定したホワイトリストのユーザのみがアクセスできます。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） ホワイト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。

ステップ 2 メンバー専用のルームかどうかをルーム所有者が変更できるように設定する場合は、[ルームがメンバー専用かどうかをルーム所有者が設定できます（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。

ステップ 3 モデレータのみがルームへのユーザの招待を、行えるようにルームを設定する場合は、[モデレータのみがメンバー専用ルームにユーザを招待できます（Only moderators can invite people to members-only rooms）] 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。

ステップ 4 ルーム所有者がメンバーに他のユーザを招待できるように設定する場合は、[モデレータがユーザをメンバー専用ルームに招待できるかどうかをルーム所有者が変更できます（Room owners can change whether or not only moderators can invite people to members-only rooms）] 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。

ステップ 5 すべてのユーザがルームへの入室をいつでも要求できるようにルームを設定する場合は、[ユーザは自分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）]

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。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。

ステップ 6 ステップ 5 に記載されている設定をルーム所有者がいつでも変更できるようにルームを設定する場合は、[ユーザが自分をメンバーとしてルームに追加できるかどうかをルーム所有者が変更できます（Room owners can change whether users can add themselves to rooms as members）] 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。

ステップ 7 [保存（Save）]をクリックします。

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

ステップ 1 ユーザが現在、オフラインであっても、ユーザをルームの参加者として保持する場合は、[メンバーと管理者はルームに入室していなくてもルームに表示されます（Members and administrators who are not in a room are still visible in 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。

ステップ 2 メンバーまたは管理者の可視性をルーム所有者が変更できるようにする場合は、[ルームに入室していないメンバーと管理者をルームに表示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 members and administrators who are not in a room are still visible in 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。

ステップ 3 以前の Group Chat 1.0 クライアントでサービスを正常に動作させるには、[ルームに古いクライアントとの下位互換性があります（Rooms are backwards-compatible with older clients）] 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。

ステップ 4 チャットルームの下位互換性をルーム所有者が管理できるようにする場合は、[ルームに古いクライアントとの下位互換性があ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 backwards-compatible with older clients）] 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。

ステップ 5 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、[デフォルトでルームは匿名になっています（Rooms are anonymous by default）] 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。

ステップ 6 ユーザの Jabber ID の匿名レベルをルーム所有者が管理できるようにする場合は、[ルームが匿名かどうかをルーム所有者が変更できます（Room owners can change whether or not rooms are anonymous）] 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。

ステップ 7 [保存（Save）] をクリックします。

招待の設定

招待の設定によって、誰がユーザの役割に基づいてユーザをルームに招待できるかを決定します。役割は、モデレータからビジターへの階層に存在するため、たとえば、参加者はビジターができることは何でも実行でき、モデレータは参加者ができることは何でも実行できます。

手順

ステップ 1 [他のユーザをルームに招待するためにユーザに必要な最小参加レベル（Lowest participation level a user can have to invite others to the room）] 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。

- [ビジター（Visitor）] を選択すると、ビジター、参加者、およびモデレータは他のユーザをルームに招待できます。
- [参加者（Participant）] を選択すると、参加者およびモデレータは他のユーザをルームに招待できます。これがデフォルトの設定です。
- [モデレータ（Moderator）] を選択すると、モデレータのみが他のユーザをルームに招待できます。

ステップ 2 招待状を送信できる最小参加者レベルの設定をルーム所有者が変更できるようにするには、[他のユーザをルームに招待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 invite others to the room）] 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。

ステップ 3 [保存（Save）] をクリックします。

利用者数の設定

手順

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

手順

ステップ 1 [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（Lowest participation level a user can have to send a private message from within the room）] 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。

- [ビジター（Visitor）] を選択すると、ビジター、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。これがデフォルトの設定です。
- [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。

ステップ 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。

ステップ 3 [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（Lowest participation level a user can have to change a room's subject）] 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。

ステップ 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。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。

ステップ 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。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。

ステップ 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。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。

ステップ 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

ステップ 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。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。

ステップ 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。

ステップ 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、履歴クエリー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

ステップ 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。

ステップ 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。

ステップ 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。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。

ステップ 4 [保存（Save）] をクリックします。

第 14 章

エンド ユーザの設定と処理

IM and Presence Service のエンド ユーザの設定と処理

IM and Presence Service エンド ユーザ用の許可ポリシーを設定し、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を実行するだけでなく、重複しているエンドユーザインスタンスや無効なエンド ユーザ インスタンスを管理できます。

IM and Presence Service ノードへユーザを割り当てて、エンド ユーザを IM and Presence Service 用に設定する手順については、次のガイドを参照してください。

- 『*Cisco Unified Communications Manager Administration Guide*』
- 『*Cisco Unified Communications Manager Bulk Administration Guide*』
- 『*Installing Cisco Unified Communications Manager*』

IM and Presence Service の許可ポリシーの設定

IM and Presence Service の自動許可

IM and Presence Service は、ローカル企業の 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 サブスクリプション要求を許可します。SIP ベースのクライアントを実行するローカルユー

ザは、クライアントでこれらの登録を許可するよう求められることなく、ローカル企業の連絡先の可用性ステータスを自動的に受信します。IM and Presence Service は、連絡先がユーザの拒否リストに存在する場合にのみ、ローカル企業の連絡先の登録を許可するようにユーザに求めます。これは、IM and Presence Service における SIP ベースのクライアントのデフォルト許可動作であり、この動作を設定することはできません。

XMPP ネットワークでは、クライアントにすべてのプレゼンス サブスクリプションを送信するのがノードの標準動作で、クライアントは登録を許可または拒否するようにユーザに求めます。SIP ベースのクライアントと XMPP ベースのクライアントが混在する IM and Presence Service を（両方のクライアント タイプの許可ポリシーに合わせて）企業が展開できるように、シスコは IM and Presence Service に次の自動許可設定を提供しています。

- 自動許可をオンにすると、IM and Presence Service は、ローカル企業で XMPP ベースのクライアントおよび SIP ベースのクライアントの両方から受信したすべてのプレゼンス サブスクリプション要求を自動的に許可します。これは、IM and Presence Service におけるデフォルト設定です。
- 自動許可をオフにすると、IM and Presence Service は XMPP ベースのクライアントのみをサポートします。XMPP ベースのクライアントでは、IM and Presence Service はクライアントにすべてのプレゼンス サブスクリプションを送信し、クライアントはユーザにプレゼンス サブスクリプションを許可または拒否するよう求めます。SIP ベースのクライアントは、自動許可をオフにすると、IM and Presence で正しく動作しません。

注意 自動許可をオフにした場合、SIP ベースのクライアントはサポートされません。自動承認をオフにしたときの XMPP ベースのクライアントだけがサポートされます。

ユーザ ポリシーおよび自動許可

自動許可ポリシーの読み取りに加えて、IM and Presence サービスはプレゼンス サブスクリプション要求の処理方法を判断するためにユーザのポリシー設定を読み取ります。ユーザは Cisco Jabber クライアントからポリシー設定をします。ユーザ ポリシーには次の設定オプションがあります。

- [拒否リスト（Blocked list）]：ユーザの実際のステータスに関係なく使用不可としてユーザのプレゼンス ステータスを常に表示するローカルおよび外部（フェデレーション）ユーザのリスト。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（Allowed list）]：可用性を表示することをユーザが許可したローカルおよび外部ユーザのリスト。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（Default policy）]：ユーザのデフォルト ポリシー設定。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。

自動許可をオフにした場合、IM and Presence サービスは他のユーザの連絡先リストに存在するユーザの登録要求を自動的に許可することに注意してください。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。次に、例を示します。

- UserA は UserB のプレゼンス ステータスの表示を登録することを望んでいます。自動許可が IM and Presence サービスでオフであり、UserB は UserA の許可リストまたは拒否リストにありません。
- IM and Presence サービスは UserB のクライアント アプリケーションにプレゼンス サブスクリプション要求を送信し、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 UserB に求めます。
- UserB は、プレゼンス サブスクリプション要求を受け入れ、UserB は UserA の連絡先リストに追加されます。
- UserA は、プレゼンス サブスクリプションを許可するように求められることなく、UserB の連絡先リストに自動的に追加されます。

IM and Presence サービスは、UserB のポリシーが (i) 外部ドメインを拒否する場合、(ii) ユーザのデフォルト ポリシーがすべて拒否の場合、または (iii) [確認（Ask me）] が選択されている場合でも、UserB の連絡先リストに自動的に UserA を追加します。

ローカル IM and Presence サービス エンタープライズとサポートされる外部エンタープライズとの間にドメイン間フェデレーションを展開すると、IM and Presence サービスは、外部連絡先から受信したプレゼンス サブスクリプション要求に自動許可設定を適用しません。ただし、ユーザがその外部連絡先またはドメインにポリシーを適用した場合を除きます。外部連絡先からプレゼンス サブスクリプション要求を受信すると、ユーザが [確認（Ask me）] を選択して外部連絡先の独自の許可/拒否ポリシーを設定するように求められた場合、および外部連絡先またはドメインがユーザの許可リストまたは拒否リストにない場合にのみ、IM and Presence サービスはクライアント アプリケーションに登録要求を送信します。クライアント アプリケーションは、ユーザに登録を許可または拒否するように求めます。

（注） IM and Presence サービスは、可用性およびインスタント メッセージの両方に共通ユーザ ポリシーを使用します。

関連トピック

http://www.cisco.com/en/US/products/ps6837/products_user_guide_list.html

IM and Presence Service の構成ガイド

IM and Presence サービスの許可ポリシーの設定

IM and Presence サービスがローカル エンタープライズで XMPP ベースのクライアントおよび SIP ベースのクライアントの両方から受信したすべてのプレゼンス サブスクリプション要求を自動的に許可するようにするには、自動許可をオンにします。自動許可をオフにする場合、IM and Presence サービスが XMPP ベースのクライアントのみをサポートし、プレゼンス サブスクリプションの許可または拒否を求めるユーザ クライアントにすべてのプレゼンス サブスクリプションを送信します。

ヒント　このウィンドウ内のすべてのパラメータの定義については Cisco Unified CM IM and Presence の管理インターフェイスのオンライン ヘルプ トピックを参照してください。

手順

ステップ 1　[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] を選択します。

ステップ 2　認可ポリシーを設定します。次のいずれかの操作を実行します。

- 自動許可をオンにするには、[確認プロンプトなしで他のユーザの可用性表示を許可する（Allow users to view the availability of other users without being prompted for approva）] のチェックボックスをオンにします。
- 自動承認をオフにするには、[確認プロンプトなしで他のユーザの可用性表示を許可する（Allow users to view the availability of other users without being prompted for approval）] のチェックボックスをオフにします。

ステップ 3　[保存（Save）] をクリックします。

ステップ 4　Cisco XCP Router サービスを再起動します。

次の作業

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。

関連トピック

Cisco XCP ルータ サービスの再起動, （68 ページ）
IM and Presence Service の IM 設定, （152 ページ）

ユーザ連絡先 ID の一括名前変更

IM and Presence サービスの一括割り当てツール（BAT）により、ある形式から別の形式にユーザ連絡先リストのコンタクト ID（JID）の名前変更ができます。たとえば、firstname.lastname @ domain.com から userid @ domain.com にユーザの連絡先 ID の名前変更ができます。また、一括管理ツールは新しいコンタクト ID で各ユーザの連絡先リストを更新します。

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 Guide*』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。

このジョブを実行する前に、連絡先 ID のリストおよびそれらの連絡先 ID の対応する新しい形式を含むファイルをアップロードする必要があります。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。

<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。

Release 10.0 より、<Contact ID> は [プレゼンス トポロジ ユーザ 管理（Presence Topology User Assignment ）] **ウィンドウ**で表示されるユーザの 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
```

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 の名前を変更するには、次の手順を実行します。

手順

ステップ 1 すべての連絡先リスト内で名前を変更する連絡先 ID のリストを含んだ CSV ファイルをアップロードします。 次の手順を実行します。

a) 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（Cisco Unified CM IM and Presence Administration）] > [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) [新規追加（Add New）] をクリックします。

c) [参照（Browse）] をクリックして、CSV ファイルを検索し選択します。

d) ターゲットとして [連絡先（Contacts）] を選択します。

e) 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。

f) [保存（Save）] をクリックして、ファイルをアップロードします。

ステップ 2 パブリッシャ ノードで、[Cisco Unified CM IM and Presence 管理（Cisco Unified CM IM and Presence Administration）] > [一括管理（Bulk Administration）] > [連絡先リスト（Contact List ）] > [連絡先の名前変更（Rename Contacts）]を選択します。

ステップ 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。

ステップ 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。

ステップ 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。

ユーザ連絡先リストの一括エクスポート

IM and Presence サービスの一括管理ツール（BAT）を使用すると、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をCSVデータ ファイルにエクスポートできます。その後、BAT を使用して、ユーザ連絡先リストを別のクラスタ内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できます。BAT のユーザ連絡先リストのエクスポートおよびインポート機能を使用すると、クラスタ間でのユーザの移動が容易になります。詳細については、ユーザ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。

（注） 連絡先リスト上の、IM アドレスを持たないユーザは、エクスポートされません。

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>
```

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
User 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。
ユーザのドメイン名（User Domain）	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 であり、example.com は、ユーザのドメインです。 **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。
Contact ID	連絡先リスト エントリのユーザ ID。
Contact Domain	連絡先リスト エントリのプレゼンス ドメイン。
Nickname	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。
Group Name	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。

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
```

次の手順を実行して、BAT でユーザ連絡先リストをエクスポートし、エクスポート ファイルをダウンロードします。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [一括管理（Bulk Administration）] > [連絡先リスト（Contact List）] > [エクスポート（Export）] を選択します。

ステップ 2 連絡先リストをエクスポートするユーザを検索するには、選択基準を使用します。ユーザの検索および選択の詳細については、Cisco Unified CM IM and Presence の管理インターフェイスのオンライン ヘルプ トピックを参照してください。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 [ファイル名（File Name）] フィールドに、CSV ファイルの名前を入力します。

ステップ 5 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。

ステップ 6 [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。

ステップ 7 ジョブの実行後、エクスポート ファイルをダウンロードするには、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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。

ステップ 8 ダウンロードするエクスポート ファイルを探し、選択します。

ステップ 9 [選択項目のダウンロード] をクリックします。

ユーザ連絡先リストの一括インポート

IM and Presence Service の一括割り当てツール（BAT）を使用して、ユーザ連絡先リストを IM and Presence Service にインポートできます。このツールを使用すると、新しい IM and Presence Service クライアント ユーザの連絡先リストを事前に設定したり、既存の連絡先リストに追加したりできます。ユーザ連絡先リストをインポートするには、ユーザ連絡先リストを含む入力ファイルを BAT に指定する必要があります。

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>
```

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
```

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。

表 *27*：入力ファイルのパラメータの説明

パラメータ	説明
User 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。
ユーザのドメイン名（User Domain）	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。
Contact 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	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

パラメータ	説明
Nickname	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。
Group Name	これ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。

（注） 別のクラスタ内の別のノードまたはプレゼンス冗長グループにユーザを移動する場合は、BAT を使用して、選択したユーザの CSV ファイルを生成できます。詳細については、ユーザ連絡先リストの一括エクスポートに関するトピックを参照してください。

次の手順を実行して、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を確認します。
- BAT を使用して入力ファイルをアップロードします。
- 新しい一括管理ジョブを作成します。
- 一括管理ジョブの結果を確認します。

はじめる前に

ユーザ連絡先リストをインポートする前に、次の手順を実行する必要があります。

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。

連絡先リストの最大サイズの確認

連絡先リストを IM and Presence Service にインポートする前に、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。[連絡先リストの最大サイズ（Maximum Contact List Size）] のシス

テム デフォルト値は 200、[ウォッチャの最大数（Maximum Watchers）] のシステム デフォルト値は 200 です。

ユーザ連絡先リストを IM and Presence Service にインポート中は [連絡先リストの最大サイズ（Maximum Contact List Size）] と [ウォッチャの最大数（Maximum Watchers）] の設定値を [無制限（Unlimited）] に設定することを推奨します。これにより、移行した各ユーザ連絡先リストが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、[連絡先リストの最大サイズ（Maximum Contact List Size）] と [ウォッチャの最大数（Maximum Watchers）] の設定値を必要な値にリセットできます。

（注） 連絡先リストのインポート時に BAT を使用するとデータを損失することなく連絡先リストの最大サイズを超過できますが、 [連絡先リストの最大サイズ（Maximum Contact List Size）] の設定値を一時的に大きくするか、値を [無制限（Unlimited）] に設定してインポートすることを推奨します。インポートが完了した後に、最大値をリセットできます。

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。

次の作業

BAT を使用して入力ファイルをアップロードします。

関連トピック

ユーザごとの連絡先リストの最大サイズの設定, （151 ページ）
ユーザごとの最大ウォッチャ数の設定, （152 ページ）

BAT を使用した入力ファイルのアップロード

次の手順では、BAT を使用して CSV ファイルをアップロードする方法について説明します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [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。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 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。

ステップ 4 ターゲットとして [連絡先リスト（Contact Lists）] を選択します。

ステップ 5 トランザクション タイプとして [ユーザの連絡先 - カスタム ファイル（Import Users' Contacts – Custom File）] を選択します。

ステップ 6 [保存（Save）] をクリックし、ファイルをアップロードします。

次の作業

新しい一括管理ジョブを作成します。

新しい一括管理ジョブの作成

次の手順では、Cisco Unified CM IM and Presence の管理の新しい一括管理ジョブを作成する方法について説明します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [一括管理（Bulk Administration）]> [連絡先リスト（Contact List）]> [更新（Update）] を選択します。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

次の作業

一括管理ジョブの結果を確認します。

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。

手順

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [一括管理（Bulk Administration）] > [ジョブ スケジューラ（Job Scheduler）] を選択します。

ステップ 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。

ステップ 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。

重複するユーザ ID とディレクトリ URI の管理

Cisco IM and Presence Data Monitor サービスは、すべての IM and Presence Service クラスタ間ノードで重複するユーザ ID と、空または重複するディレクトリ UIR を確認します。何らかのエラーが検出された場合、M and Presence Service はソフトウェアでアラームを生成します。それらのエラーを修正するための対策をすぐに講じて、ユーザに対する通信の中断を回避することを推奨します。

Cisco Unified CM IM and Presence の管理 GUI を使用して、システム トラブルシュータから重複するユーザ ID やディレクトリ URI のチェックの状態を監視できます。また、GUI を使用して、ユーザ ID と ディレクトリ URI のチェック間隔を設定できます。

これらのアラームの原因となったユーザに関する特定の情報を収集するには、コマンドラインインターフェイスを使用します。システム アラームやアラートを監視するには、リアルタイム監視ツール（RTMT）を使用します。

コマンド ライン インターフェイスを使用したユーザ ID またはディレクトリ URI の検証の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。リアルタイム監視ツールの使用の詳細については、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。

ユーザ ID と ディレクトリ URI モニタリング

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。

Cisco Unified CM IM and Presence 管理 GUI のシステム トラブルシュータを使用することで、重複ユーザ ID とディレクトリ URI チェックのステータスを監視することができます。これらのユーザ ID とディレクトリ URI チェックの間隔は、Cisco Unified CM IM and Presence 管理 GUI を使用して設定されます。有効な範囲は、5 ～ 1440 分（12 時間）です。デフォルトは 30 分です。

エラーが検出された場合、IM and Presence Service ではソフトウェア アラームが発生します。

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、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。

ユーザ ID と ディレクトリ URI のエラー状態

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 *28*：ユーザ *ID* と ディレクトリ *URI* のエラー状態

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。

エラー状態	説明	推奨措置
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**： • `DuplicateUserid` • `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。
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 ID と ディレクトリ URI の確認と変更

特に、新しいユーザを追加した後や連絡先リストを移行した場合は、システムでアラームが発生するのを待たずに、重複ユーザ情報のチェックを実行することを推奨します。

Cisco Unified CM IM and Presence の管理 GUI のシステム トラブルシュータを使用すると、ユーザ ID とディレクトリ URI のエラーの概要を表示できます。詳細および包括的なレポートについては、CLI コマンドを使用し、IM and Presence Service ユーザを検証します。

ユーザに重複または無効な情報があると特定された場合は、**[エンド ユーザ設定（End User Configuration）]** ウィンドウ（[ユーザ管理（User Management）] > [エンド ユーザ（EndUser）]）を使用して、Cisco Unified Communications Manager のユーザ レコードを変更できます。必要に応じて、すべてのユーザに有効なユーザ ID またはディレクトリ URI 値があることを確認します。詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

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。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 チェック間隔の設定

Cisco Unified CM IM and Presence の管理を使用して、重複ユーザ ID とディレクトリ URI の展開ですべてのノードとクラスタを確認するために Cisco IM and Presence Data Monitor サービスの間隔を設定します。

整数を使用して間隔を分単位で入力します。値の範囲は5～1440です。デフォルトは30分です。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [サービス パラメータ（Service Parameters）] を選択します。

ステップ 2 [サービス（Service）] フィールドの [Cisco IM and Presence データ モニタ（Cisco IM and Presence Data Monitor）] を選択します。

ステップ 3 [ユーザ確認間隔（User Check Interval）] として 5 ～ 1440 の整数を入力し、[保存（Save）] をクリックします。

システム トラブルシュータを使用したユーザ ID とディレクトリ URI の検証

Cisco Unified CM IM and Presence Administration の GUI のシステム トラブルシュータを使用して、展開されているすべてのノードおよびクラスタ全体にわたって重複するユーザ ID や、重複または無効なディレクトリ URI を特定するシステム チェックのステータスを表示します。

詳細および包括的なレポートについては、CLI コマンドを使用し、IM and Presence Service ユーザを検証します。CLI の使用方法およびコマンドの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [診断（Diagnostics）] > [システム トラブルシュータ（System Troubleshooter）] を選択します。

ステップ 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。

重複または無効なユーザ情報が検出された場合は、推奨ソリューションを実行します。ユーザ ID およびディレクトリ URI のエラーのトラブルシューティングを行うには、トラブルシューティングに関するトピックを参照してください。

ヒント [ソリューション（Solution）] 列の [修正（fix）] リンクをクリックすると、Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration） の **[エンドユーザの設定（End User Configuration）]** ウィンドウにリダイレクトされます。このウィンドウで、ユーザ プロファイルを見つけ、再設定することができます。詳細なユーザ検証情報については、CLI コマンドを使用してユーザを検証します。

（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。

関連トピック

重複したユーザ ID エラーの受信, （271 ページ）
重複または無効なディレクトリ URI エラーの受信, （272 ページ）

第 15 章

ユーザの移行

IM and Presence Service クラスタ間のユーザの移行

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。次の手順を記述されている順に完了する必要があります。

1. 現在のクラスタから移行ユーザの割り当てを解除します。
2. 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。
3. Cisco Unified Communications Manager から現在のホーム クラスタの IM and Presence Service および Cisco Jabber の移行ユーザを無効にします。
4. LDAP 同期が Cisco Unified Communications Manager で有効になっている場合
   - 新しいクラスタが情報を同期する新しい組織ユニットにユーザを移動します。
   - 新しいホーム Cisco Unified Communications Manager にユーザを同期します。
5. LDAP 同期が Cisco Unified Communications Manager で有効になっていない場合は、手動で Cisco Unified Communications Manager の移行ユーザをプロビジョニングします。
6. IM and Presence Service および Cisco Jabber のユーザを有効にします。
7. 移行されたユーザの連絡先リストのデータを復元するために、新しいホームクラスタに連絡先リストをインポートします。

はじめる前に

次のタスクを実行します。

- 現在のクラスタおよび新しいホームクラスタの完全な DRS を実行します。詳細については、『*Disaster Recovery System Administration Guide*』を参照してください。
- 次のサービスが実行されていることを確認します。

- Cisco Intercluster Sync Agent
- Cisco AXL Web Service
- Cisco Sync Agent

- トラブルシュータを実行し、Intercluster Sync Agent の問題が報告されないことを確認します。この手順を続行する前に、トラブルシュータで報告されたすべての Intercluster Sync Agent の問題を解決する必要があります。
- [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 ）] 設定を有効にすることを推奨します。この設定を有効にするには、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] を選択します。この設定の変更には、Cisco XCP Router を再起動する必要があります。
- 次の設定を [無制限（No Limit）] に設定することを推奨します。
  - 連絡先リストの最大サイズ（ユーザごと）（Maximum Contact List Size (per user)）
  - ウォッチャの最大数（ユーザごと）（Maximum Watchers (per user)）

    これらの設定を行うには、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] を選択します。
- 移行されるユーザに現在の（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。これらのユーザに他のクラスタでライセンスが供与されている場合、次の手順に進む前に完全ライセンスが供与されている必要はありません。

現在のクラスタからのユーザ割り当ての解除

現在のクラスタから移行ユーザの割り当てを解除するには、次の手順を実行します。

手順

ステップ 1 [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）] を選択します。

ステップ 2 リモート IM and Presence クラスタに移行するユーザを選択します。

ステップ 3 [選択されたユーザの割り当て（Assign Selected Users）] を選択し、次のダイアログボックスで [未割り当て（Unassigned）] を選択します。

ステップ 4 [保存（Save）] をクリックします。

次の作業

ユーザ連絡先リストのエクスポートに進みます。

ユーザ連絡先リストのエクスポート

現在のクラスタから移行の連絡先リストをエクスポートするには、次の手順を実行します。

手順

ステップ 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 の管理（Cisco Unified CM IM and Presence Administration）] > [一括管理（Bulk Administration）] > [連絡先リスト（Contact List）] > [エクスポート（Export）] を選択します。

b) [クラスタ内のすべての未割り当てユーザ（All unassigned users in the cluster）] を選択し、[Find（検索）] をクリックします。

c) 結果を確認し、必要に応じて [および/また（AND/OR）] 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) リストが完了すると、[次へ（Next）] 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。

ステップ 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 の管理（Cisco Unified CM IM and Presence Administration）] > [一括管理（Bulk Administration）] > [ジョブ スケジューラ（Job Scheduler）] 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) 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。タイムスタンプがファイル名に付加されることに注意してください。

e) [ジョブの結果（Job Results）] 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。ジョブの開始時刻と終了時刻が一覧表示され、ジョブの結果の要約が表示されます。

ステップ 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 の管理（Cisco Unified CM IM and Presence Administration）] > [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（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。

次の作業

ユーザを非ライセンスに設定します。

IM and Presence Service のユーザの無効化

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。

ユーザを一括更新する方法については、『*Cisco Unified Communications Manager Bulk Administration Guide*』を参照してください。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] > [ユーザ管理（User Management）] > [エンド ユーザ（End User）] を選択します。

ステップ 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。

ステップ 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。

ステップ 4 [保存（Save）] をクリックします。

新しいクラスタへのユーザの移動

新しいクラスタにユーザを移動する手順は、LDAP 同期が Cisco Unified Communications Manager で有効になっているかどうかによって異なります。

Cisco Unified Communications Manager で有効な LDAP 同期

LDAP 同期が Cisco Unified Communications Manager で有効になっている場合は、新しい組織ユニットにユーザを移動し、新しいホーム クラスタにユーザを同期する必要があります。

新しい組織ユニットへのユーザの移動

LDAP 同期が Cisco Unified Communications Manager で有効になっている場合は、展開でクラスタごとに異なる LDAP 構造が使用されるときに（OU 分割）、新しいクラスタの同期元となる新しい組織ユニット（OU）にユーザを移動する必要があります。この場合、ユーザは LDAP からそのホーム クラスタにのみ同期されます。

（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。

新しいホーム クラスタの関連する OU に移行ユーザを移動する方法の詳細については、LDAP 管理マニュアルを参照してください。

ユーザの移動後、古い LDAP のクラスタから LDAP エントリを削除する必要があります。

次の作業

新しいホーム クラスタへのユーザの同期に進みます。

新しいホーム クラスタへのユーザの同期

LDAP が Cisco Unified Communications Manager になっている場合、新しいホーム Cisco Unified Communications Manager クラスタにユーザを同期する必要があります。Cisco Unified Communications Manager でこれを手動で同期するか、Cisco Unified Communications Manager でスケジュールされた同期化が行われるまで待機できます。

Cisco Unified Communications Manager で、同期を手動で強制するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified CM の管理で、[システム（System）] > [LDAP（LADP）] > [LDAP ディレクトリ（LDAP Directory）] を選択します。

ステップ 2 [完全同期を今すぐ実施（Perform Full Sync Now）] をクリックします。

次の作業

IM and Presence サービスのユーザを有効にし、新しいクラスタのユーザにライセンスを供与する手順に進みます。

関連トピック

新しいクラスタの IM and Presence サービスのユーザの有効化, （248 ページ）

Cisco Unified Communications Manager で有効ではない LDAP 同期

LDAP 同期が Cisco Unified Communications Manager で有効になっていない場合、新しい Cisco Unified Communications Manager クラスタでユーザを手動でプロビジョニングする必要があります。詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

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

ステップ 1 Cisco Unified CM の管理で、[ユーザの管理（User Management）] > [エンド ユーザ（End User）] を選択します。

ステップ 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。

ステップ 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。

ステップ 4 [保存（Save）] をクリックします。

ステップ 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、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

ユーザを一括更新する方法については、『*Cisco Unified Communications Manager Bulk Administration Guide*』を参照してください。

次の作業

新しいホーム クラスタの連絡先リストのインポートに進みます。

ホーム クラスタでの連絡先リストのインポート

移行されたユーザの連絡先データを復元するには、連絡先リストをインポートする必要があります。

手順

ステップ 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 の管理（Cisco Unified CM IM and Presence Administration）] > [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) [新規追加（Add New）] 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) [保存（Save）] をクリックして、ファイルをアップロードします。

ステップ 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 の管理（Cisco Unified CM IM and Presence Administration）] > [一括管理（Bulk Administration）] > [連絡先リスト（Contact List）] > [更新（Update）] 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。

ステップ 3 連絡先リストのインポート ステータスをモニタします。

a) [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [一括管理（Bulk Administration）] > [ジョブ スケジューラ（Job Scheduler）] 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。

第 16 章

IM and Presence Service の多言語サポート設定

ロケールのインストール

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 サービス 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。これらのファイルは、次のファイル名の表記を使用します。

- 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） シスコ承認の Cisco Unified Communications Manager の仮想化導入の顧客が提供するサーバは複数のロケールをサポートできます。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。

ロケールのインストールに関する考慮事項

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 サービス 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については、『*Upgrade Guide for Cisco Unified Communications Manager*』を参照してください。

ロケール ファイル

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 サービス 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。

ノードでロケールをインストールする時は、次のファイルをインストールします。

- ユーザ ロケール ファイル：これらのファイルには、特定の言語と国の言語情報が含まれています。次の表記法が使用されます。

  `cm-locale-language-country-version.cop`（Cisco Unified Communications Manager）

  ps-locale-language_country-version.cop（IM and Presence Service）

- 複合ネットワーク ロケール ファイル：すべての国に対応した、さまざまなネットワーク項目（電話機のトーン、Annunciator、およびゲートウェイ トーンなど）の国固有のファイルが格納されています。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）

IM and Presence Service へのロケール インストーラのインストール

はじめる前に

- 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。
- 変更を有効にするためには、サーバを再起動する必要があります。ロケールのインストール手順がすべて完了したら、クラスタ内の各サーバを再起動してください。クラスタ内のすべてのサーバを再起動するまで、システム内で更新は行われません。サーバの再起動後にサービスが再開されます。

手順

ステップ 1 cisco.com に移動し、IM and Presence Service 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

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6 [Software Upgrades（ソフトウェア アップグレード）] > [Install/Upgrade（インストール/アップグレード）]を選択します。

ステップ 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。

ステップ 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。

ステップ 9 [サーバ（Server）] フィールドに IM and Presence Service のサーバ名を入力します。

ステップ 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。

ステップ 11 [転送プロトコル（Transfer Protocol）] で [SFTP（SFTP）] を選択します。

ステップ 12 [次へ（Next）] をクリックします。

ステップ 13 検索結果のリストから IM and Presence Service ロケール インストーラを選択します。

ステップ 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。

ステップ 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。

ステップ 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。

（注） IM and Presence Service は現在 Safari ブラウザをサポートしていません。

a) Internet Explorer バージョン 6.x を使用する場合は、次の手順を実行します。

1. [ツール（Tools）] > [インターネット オプション（Internet Options）] を選択します。
2. [一般（General）] タブを選択します。
3. [言語（Languages）] をクリックします。
4. [上へ（Move Up）] ボタンを使用して、優先する言語をリストの先頭に移動します。
5. [OK] をクリックします。

b) Mozilla Firefox バージョン 3.x を使用する場合は、次の手順を実行します。

1. [ツール（Tools）] > [オプション（Options）] を選択します。
2. [コンテンツ（Content）] タブを選択します。
3. [言語（Languages）] セクションの [選択（Choose）] をクリックします。
4. [上へ（Move Up）] ボタンを使用して、優先する言語をリストの先頭に移動します。
5. [OK] をクリックします。

ステップ 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 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 *29*：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。
[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。

メッセージ	説明
[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 *30*：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 V 部

IM and Presence Service のトラブルシューティング

第 17 章

高可用性のトラブルシューティング

プレゼンス冗長グループのノードのステータスの表示

[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、プレゼンス冗長グループのメンバーになっている IM and Presence サービス ノードのステータスを表示します。

手順

ステップ 1 [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。
[プレゼンス冗長グループの検索/一覧表示(Find and List Presence Redundancy Groups)] ウィンドウが表示されます。

ステップ 2 プレゼンス冗長グループの検索パラメータを選択して、[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。

ステップ 3 検索結果に一覧表示されているプレゼンス冗長グループを選択します。
[プレゼンス冗長グループの設定(Presence Redundancy Group Configuration)] ウィンドウが表示されます。そのグループ内で 2 つのノードが設定され、高可用性が有効になっている場合、[高可用性(High Availability)] 領域にそのグループ内のノードのステータスが表示されます。

ノード状態の定義

表 *31*：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)]	これは、Cisco Server Recovery Manager サービスが開始されたときの初期（遷移）状態であり、一時的な状態です。
[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されると、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 サービス ノードが可用性 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。
[標準（Normal）]	これは安定した状態です。IM and Presence サービス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)]	これは安定した状態です。IM and Presence サービス ノードが、そのピア 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）ノードに移動しました。
[テイクオーバー中(Taking Over)]	これは遷移状態です。IM and Presence サービス ノードが、そのピア ノードへのテイクオーバー中です。
[フェールオーバー中(Failing Over)]	これは遷移状態です。IM and Presence サービス ノードが、そのピア ノードによってテイクオーバーされているところです。
[フェールオーバー済み(Failed Over)]	これは安定した状態です。IM and Presence サービス 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/重要なサービスが実行されていません(Failed Over with Critical Services Not Running)]	これは安定した状態です。IM and Presence サービス ノード上の重要なサービスの一部が、停止したか失敗しました。

状態	説明
[フォールバック中(Falling Back)]	これは遷移状態です。システムが、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 ノードへのフォールバック中です。
[テイクバック中(Taking Back)]	これは遷移状態です。失敗した IM and Presence サービス ノードが、そのピアからテイクバックされているところです。
[失敗モードで実行中(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。 原因として、IM and Presence サービス ノード上で高可用性が正しく有効にされなかったことが考えられます。プレゼンス冗長グループの両方のノード上で、Server Recovery Manager サービスを再起動してください。

ノードの状態、原因、および推奨処置

[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 *32*：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/推奨処置
[標準（Normal）]	[標準（Normal）]	[標準（Normal）]	[標準（Normal）]	[標準（Normal）]
[フェールオーバー中(Failing Over)]	管理者からの要求時	[テイクオーバー中(Taking Over)]	管理者からの要求時	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）]	管理者からの要求時	[バックアップモードで実行中(Running in Backup Mode)]	管理者からの要求時	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/推奨処置
[テイクバック中(Taking Back)]	管理者からの要求時	[フォールバック中(Falling Back)]	管理者からの要求時	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)]	管理者からの要求時	ノード 1 が「アイドル」状態であるとき、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が手動フェールオーバーモードであるとき、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、両方のノード上の SRM サービスを再起動しました。
[アイドル（Idle）]	管理者からの要求時	[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 モードで実行中でも、ノード 1 のハートビートがタイムアウトする前に、管理者がノード 2 上の SRM サービスを再起動しました。
[フェールオーバー中(Failing Over)]	管理者からの要求時	[テイクオーバー中(Taking Over)]	初期化	ノード 2 がテイクオーバー中でも、ノード 1 のハートビートがタイムアウトする前に、管理者がノード 2 上の 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)]	管理者からの要求時	ノード 1 がテイクバック中でも、ノード 2 のハートビートがタイムアウトする前に、管理者がノード 1 上の 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 [正常(Normal)] 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/推奨処置
[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 [フェールオーバー済み(Failed Over)] 状態に遷移します。 • ノード 1 のリブートにより、重要なサービスが稼働状態に戻る。 • ノード 1 が [フェールオーバー済み/重要なサービスが実行されていません(Failed Over with Critical Services Not Running)] 状態であるとき、管理者がノード 1 上で重要なサービスを開始する。 ノード 1 が [フェールオーバー済み(Failed Over)] 状態に遷移するとき、プレゼンス冗長グループのノードを [正常(Normal)] 状態に復元するために、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。
[フェールオーバー済み/重要なサービスが実行されていません(Failed Over with Critical Services not Running)]	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 上で重要なサービスがダウンしています。IM and Presence サービスは、ノード 2 への自動フェールオーバーを実行します。 **推奨処置**： **1** ノード 1 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、手動でのそのサービスの開始を試みます。 **2** ノード 1 上の重要なサービスが開始されない場合は、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起動して実行中になったら、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 [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/推奨処置
[フェールオーバー済み/重要なサービスが実行されていません(Failed Over with Critical Services not Running)]	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 上のデータベース サービスがダウンしています。IM and Presence サービスは、ノード 2 への自動フェールオーバーを実行します。 **推奨処置**： **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起動して実行中になったら、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 [正常(Normal)] 状態に復元します。
[失敗モードで実行中(Running in Failed Mode)]	重要なサービスの開始が失敗	[失敗モードで実行中(Running in Failed Mode)]	重要なサービスの開始が失敗	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上で、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)] ウィンドウで [リカバリ(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起動して実行中になったら、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 [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/推奨処置
[失敗モードで実行中(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 ノード上で重要なサービスがダウンしました。両方のノードが失敗状態に入ります。 **推奨処置**： **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 [リカバリ(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失われているためにノード 1 がダウンしているか、SRM サービスが実行されていません。		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 からのハートビートを見失いました。IM and Presence サービスは、ノード 2 への自動フェールオーバーを実行します。 **推奨処置。** 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、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。[プレゼンス冗長グループの設定(Presence Redundancy Group Configuration)] ウィンドウで [リカバリ(Recovery)] をクリックして、ノードを「通常」状態に復元します。 **2** SRM サービスを開始し、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 [正常(Normal)] 状態に復元します。 **3** （ノードがダウンしている場合）ノード 1 を修復し、電源を入れます。 **4** ノードが起動し、すべての重要なサービスが実行中になったら、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 [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/推奨処置
（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 がダウンしています。		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 上で次のような条件が発生したため、IM and Presence サービスはノード 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 **推奨処置**： **1** ノード 1 を修復し、電源を入れます。 **2** ノードが起動し、すべての重要なサービスが実行中になったら、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 [正常(Normal)] 状態に復元します。
[フェールオーバー済み/重要なサービスが実行されていません (Failed Over with Critical Services not Running)] または [フェールオーバー完了 (Failed Over)]	初期化	[バックアップモード (Backup Mode)]	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。 **推奨処置**： ノード 1 が起動し、すべての重要なサービスが実行中になったら、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 [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/推奨処置
[失敗モードで実行中(Running in Failed Mode)]	Cisco Server Recovery Manager によるユーザのテイクオーバーが失敗	[失敗モードで実行中(Running in Failed Mode)]	Cisco Server Recovery Manager によるユーザのテイクオーバーが失敗	テイクオーバー プロセス中のユーザ移動は失敗します。 **推奨処置**： 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)] ウィンドウで、[リカバリ(Recovery)] をクリックしてください。問題が解決しない場合は、ノードをリブートします。
[失敗モードで実行中(Running in Failed Mode)]	Cisco Server Recovery Manager によるユーザのテイクバックが失敗	[失敗モードで実行中(Running in Failed Mode)]	Cisco Server Recovery Manager によるユーザのテイクバックが失敗	フォールバック プロセス中のユーザ移動は失敗します。 **推奨処置**： 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)] ウィンドウで、[リカバリ(Recovery)] をクリックしてください。問題が解決しない場合は、ノードをリブートします。
[失敗モードで実行中(Running in Failed Mode)]	[不明（Unknown）]	[失敗モードで実行中(Running in Failed Mode)]	[不明（Unknown）]	ノード上の SRM が再起動したがもう一方のノード上の SRM が失敗状態であるか、内部システムエラーが発生しました。 **推奨処置**： [プレゼンス冗長グループの設定(Presence Redundancy Group Configuration)] ウィンドウで、[リカバリ(Recovery)] をクリックしてください。問題が解決しない場合は、ノードをリブートします。
[バックアップがアクティブ化済み(Backup Activated)]	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(Failover Affected Services)]	データベースの自動リカバリに失敗	バックアップ ノード上でデータベースがダウンしました。ピア ノードがフェールオーバー 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行われ、すべてのユーザはプライマリ ノードに移動されます。

ノード 1		ノード 2		
状態	理由	状態	理由	原因/推奨処置
[バックアップがアクティブ化済み (Backup Activated)]	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 (Failover Affected Services)]	重要なサービスのダウンの自動リカバリ	バックアップ ノード上で重要なサービスがダウンしました。ピア ノードが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行われ、すべてのユーザはピア ノードに移動されます。
[不明（Unknown）]		[不明（Unknown）]		ノード状態は不明です。 原因として、IM and Presence サービス ノード上で高可用性が正しく有効にされなかったことが考えられます。 **推奨処置**： プレゼンス冗長グループの両方のノード上で、Server Recovery Manager サービスを再起動してください。

第 18 章

UserID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 コマンドを使用して、全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 プロファイルでのユーザ ID とディレクトリ URI フィールドは、LDAP Directory にマップされる場合があります。この場合は、LDAP Directory サーバで修正を行います。

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 コマンドを使用して、全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 プロファイルでのユーザ ID とディレクトリ URI フィールドは、LDAP Directory にマップされる場合があります。この場合は、LDAP Directory サーバで修正を行います。

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 19 章

シングル サインオンのトラブルシューティング

セキュリティ信頼エラー メッセージ

問題 シングルサインオン機能を有効にすると、「Security trust error（セキュリティ信頼エラー）」というメッセージが表示されます。

考えられる原因 IM and Presence Service ノードで OpenAM ノードが信頼されない原因としてセキュリティ証明書の問題が考えられます。

解決法 Java をインストールしたときに選択したアプローチであった場合の OpenAM 自己署名証明書、ならびに、Java をインストールしたときに選択したアプローチであった場合に OpenAM 証明書に署名したルート証明書および中間証明書が IM and Presence Service ノード、および 再起動した IM and Presence Service ノードの Tomcat サービスにアップロードされていることを確認します。また、SSO を有効にしたときに正しい OpenAM URL が GUI で指定されていることも確認する必要があります。OpenAM URL はポート番号を指定した完全修飾ドメイン名である必要があります。たとえば、`https://openam-01.corp28.com:8443/opensso` などです。

関連トピック

Java のインストール, （167 ページ）
Java のインストール, （167 ページ）

「Invalid Profile Credentials（プロファイル クレデンシャルが無効です）」メッセージ

問題 SSO を有効にすると、「Invalid Profile Credentials（プロファイル クレデンシャルが無効です）」というメッセージが表示されます。

考えられる原因 IM and Presence Service ノード J2EE エージェントに誤った名前とパスワードを指定している可能性があります。

解決法 OpenAM サーバの J2EE エージェント プロファイル用に設定された名前とパスワードの値を確認します。これらの値は、SSO を有効にするときに指定する必要があります。

関連トピック

OpenAM サーバでの J2EE エージェント プロファイルの設定, （183 ページ）

「モジュール名が無効です（ModuleNameIsInvalid）」というメッセージ

問題 シングルサインオンを有効にすると、「Module Name is Invalid（モジュール名が無効です）」というメッセージが表示されます。

考えられる原因 SSOモジュールインスタンスに誤った名前を指定している可能性があります。

解決法 SSO モジュール インスタンスを設定する手順を確認します。

関連トピック

SSO モジュール インスタンスの設定, （182 ページ）

「Invalid OpenAM Access Manager （Openam）Server URL（OpenAM Access Manager（Openam）サーバ URL が無効です）」メッセージ

問題 シングル サインオンを有効にすると、「'Invalid OpenAM Access Manager (Openam) Server URL（OpenAM Access Manager（Openam）サーバ URL が無効です）」というメッセージが表示されます。

考えられる原因 SSO を有効にしたときに GUI または CLI で指定した OpenAM URL が誤っていた可能性があります。

解決法 SSO を有効にしたときに GUI で指定した OpenAM URL が正しいことを確認します。OpenAM URL はポート番号を指定した完全修飾ドメイン名である必要があります。たとえば、`https://server1.cisco.com:8443/opensso` などです。また、OpenAM サーバが稼動中であり、OpenAM 管理 GUI にアクセスできることを保証する必要があります。

Web ブラウザに 401 エラーが表示される

問題 IM and Presence ノードの SSO 対応 Web アプリケーションにアクセスすると、Web ブラウザに HTTP 401 エラー コードが表示されます。

考えられる原因 ユーザのブラウザの設定に問題がある可能性があります。

解決法 シングル サインオン用にクライアント ブラウザを設定する手順を確認します。

関連トピック

シングル サインオン用のクライアント ブラウザ設定, （164 ページ）

Web ブラウザに 403 エラーが表示されたり、空白の画面が表示される

問題 IM and Presence Service ノードの SSO 対応 Web アプリケーションにアクセスすると、Web ブラウザに HTTP 403 エラー コードや空白の画面が表示されます。

考えられる原因 この IM and Presence Service ノード用の OpenAM ポリシーの設定に問題がある可能性があります。

解決法　この IM and Presence Service ノードの 6 個のポリシー規則をすべて追加し、すべてのポリシー規則が GET/POST アクションで有効になっていることを確認します。また、サブジェクトをポリシーに追加したことを確認する必要があります。

関連トピック

OpenAM サーバでのポリシーの設定,（179 ページ）

「User is not Authorized to Perform this Function（ユーザはこの機能を実行する権限がありません）」エラー メッセージ

問題　Web アプリケーションにアクセスし、ページにアクセスしようとすると、「User is not Authorized to Perform this Function（ユーザはこの機能を実行する権限がありません）」というメッセージが表示されます。

考えられる原因　IM and Presence Service に割り当てられているユーザの権限に問題がある可能性があります。

解決法　IM and Presence Service Web アプリケーションへのアクセスに失敗する場合は、そのユーザが、標準 *CCM* スーパー ユーザ グループ、またはこの IM and Presence Service ノードで同等な役割を持つグループのメンバーであることを確認します。

Web ブラウザに HTTP 404 エラーが表示される

問題　IM and Presence Service ノードの SSO 対応 Web アプリケーションにアクセスすると、Web ブラウザに HTTP 404 エラー コードが表示されます。

考えられる原因　この IM and Presence Service ノード用の OpenAM ポリシー設定、または OpenAM J2EE エージェントの設定のいずれかに問題がある可能性があります。

解決法　ホスト名のみを含む URL を使用してこの IM and Presence Service ノードにアクセスしようとしていないことを確認します。これは、Web アプリケーションに対して SSO が有効になっている場合はサポートされません。この IM and Presence Service ノードのポリシー ルールを確認します。また、OpenAM サーバのこの IM and Presence Service の J2EE エージェント設定にログイン処理 URI を追加したことも確認します。

関連トピック

OpenAM サーバでのポリシーの設定,（179 ページ）
OpenAM サーバでの J2EE エージェント プロファイルの設定,（183 ページ）

Web ブラウザに HTTP 500 エラーが表示されたり、空白の画面が表示される

問題 IM and Presence Service ノードの SSO 対応 Web アプリケーションにアクセスすると、Web ブラウザに HTTP 500 エラー コードや空白の画面が表示されます。

考えられる原因 この IM and Presence Service ノード用の OpenAM J2EE エージェントの設定に問題がある可能性があります。

解決法 1）このノードの J2EE エージェントのログイン処理 URL を追加したこと、および 2）[OpenAM Services] タブにログイン処理 URL を追加し、その他すべてのログイン URL を削除したことを確認します。

関連トピック

OpenAM サーバでの J2EE エージェント プロファイルの設定, （183 ページ）

「Authentication Failed（認証に失敗しました）」メッセージ

問題 IM and Presence Service ノード用の SSO 対応 Web アプリケーションにアクセスすると、「Authentication failed（認証に失敗しました）」というメッセージを示す OpenAM ログイン画面が表示されます。

考えられる原因 WindowsDesktopSSO のログイン モジュールに問題がある可能性があります。

解決法 1）すべての SSO モジュール インスタンスの設定が正しいこと、2）指定したディレクトリにキータブ ファイルが存在すること、および 3）クロックが次のデバイスに対して同期化されていることを確認します。

- **解決法** ユーザの Windows ベースのコンピュータ
- **解決法** Active Directory
- **解決法** OpenAM サーバ
- **解決法** IM and Presence Service ノード

関連トピック

SSO モジュール インスタンスの設定, （182 ページ）

Web ブラウザに OpenAM のログイン画面が表示される

問題 IM and Presence Service ノードの SSO 対応 Web アプリケーションにアクセスすると、Web ブラウザに OpenAM のログイン画面が表示されます。

考えられる原因 この IM and Presence Service ノード用の OpenAM J2EE エージェントの設定に問題がある可能性があります。

解決法 ログイン URL を [**OpenAM Services**]タブに追加し、他のすべてのログイン URL を除外したことを確認します。

関連トピック

OpenAM サーバでの J2EE エージェント プロファイルの設定, （183 ページ）

Web ブラウザに IM and Presence Service のログイン画面が表示される

問題 IM and Presence Service ノードの SSO 対応 Web アプリケーションにアクセスすると、Web ブラウザに Web アプリケーションのログイン画面が表示されます。

考えられる原因 この IM and Presence Service ノード用の OpenAM J2EE エージェントの設定に問題がある可能性があります。

解決法 この IM and Presence Service ノードの J2EE エージェントの ログイン処理 URL を追加したことを確認してください。

関連トピック

OpenAM サーバでの J2EE エージェント プロファイルの設定, （183 ページ）

ユーザ名とパスワード用の Internet Explorer のプロンプト

問題 IM and Presence Service ノード用の SSO 対応 Web アプリケーションにアクセスすると、Internet Explorer Web ブラウザがユーザ名とパスワードの入力を求めるメッセージを表示します。

考えられる原因 ユーザのブラウザの設定に問題がある可能性があります。

解決法 シングル サインオン用にクライアント ブラウザを設定する手順を確認します。

関連トピック

シングル サインオン用のクライアント ブラウザ設定, （164 ページ）

「User has no profile on this organization（ユーザにこの組織のプロファイルはありません」メッセージ

問題 IM and Presence Service ノード用の SSO 対応 Web アプリケーションにアクセスすると、Web ブラウザに「User has no profile on this organization（ユーザにこの組織のプロファイルはありません）」というメッセージが表示された OpenAM 画面が表示されます。

考えられる原因 OpenAM ユーザ プロファイルが **[無視（ignored）]** に設定されていない可能性があります。

解決法 GUI コンフィギュレータを使用して OpenAM を設定する手順を参照してください。

関連トピック

GUI Configurator を使用した OpenAM のセットアップ, （178 ページ）

SSO 有効化の問題

問題 SSO 機能を有効にできません。

考えられる原因 OpenAM サーバが展開されている Tomcat インスタンスが応答しない、または突然シャットダウンした場合は、IM and Presence Service のSSO 機能を有効にできないことがあります。SSO を IM and Presence Service で正常に有効にするには、OpenAM が動作可能である必要があります。IM and Presence は OpenAM Tomcat インスタンスを監視しません。その結果、この発生に対して IM and Presence Service アラームまたは通知は生成されません。

解決法 Cisco Unified IM and Presence オペレーティング システムの管理 GUI から SSO を有効にできない場合は、OpenAM サーバで Tomcat が実行されていることを確認します。OpenAM サーバで Tomcat が実行されていることを確認した後も問題が引き続き発生する場合は、OpenAM サーバで Tomcat を再起動し、もう一度 SSO を有効にしてみてください。

解決法 OpenAM サーバで Tomcat がクラッシュすると、OpenAM が応答不能状態になり、これが IM and Presence Service に通知されない場合があります。

証明書エラー

問題 OpenAM と IM and Presence Service 間の通信を確認するために、証明書インポート ツールを使用すると、「Verify SSL connectivity to the specified certificate server（指定した証明書サーバへの SSL 接続の確認）」テストでエラーが発生する場合があります。このテストは、「The Troubleshooter has encountered an internal error（トラブルシュータで内部エラーが検出されました）」というエラーで失敗する可能性があります。

考えられる原因　このエラーは、OpenAM/Tomcat インスタンスが HTTP コネクタを設定した方法が原因である場合があります。

解決法　次の手順を実行し、証明書のエラーを解決します。

1. OpenAM/Tomcat サーバで server.xml コンフィギュレーション ファイルを検索します。通常、このファイルには次の場所からアクセスできます。

   `C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\server.xml`

2. ポート値が 8443 の [コネクタ（Connector）] の [clientAuth] 属性の値セットを確認します。この属性が True に設定されていると、証明書インポート ツールが失敗する可能性があります。
3. [clientAuth] 属性を [want] または [false] に変更します。
4. OpenAM サーバの Tomcat サービスを再起動します。
5. 証明書インポート ツールを再実行し、IM and Presence Service に OpenAM 証明書をインポートします。
6. clientAuth 属性を元の値に戻します。
7. OpenAM サーバの Tomcat サービスを再起動します。

関連トピック

IM and Presence サービスへの OpenAM 証明書のインポート, （186 ページ）

第 20 章

IM and Presence Service のトラブルシューティングに使用するトレース

トレースを使用した IM and Presence Service のトラブルシューティング

Cisco Unified IM and Presence サービスアビリティ を使用して、IM and Presence サービス展開で問題を修復するためのトレースを開始できます。トレースを有効にした後に、Real-Time Monitoring

Tool（RTMT）またはトレースログファイルにアクセスするには、コマンドラインインターフェース（CLI） を使用します。

IM and Presence サービスでサービスアビリティ トレースを使用する手順については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。RTMT のインストールおよび使用に関する詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。トレース ログファイルにアクセスするための file list および file get などの CLI コマンド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。

ヒント　file get などの CLI コマンドを使用してファイルを転送するには、SFTP サーバのみを使用します。

IM and Presence Service ノードに共通のトレースとログ ファイルの場所

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。リアルタイム監視ツール（RTMT）を使用するか、file list や file get などのコマンド ラインインターフェイス（CLI）コマンドを使用してトレース ログ ファイルを表示できます。file get などの CLI コマンドを使用してファイル転送を行う場合は、SFTP サーバのみを使用します。RTMT のインストールおよび使用の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。トレース ログ ファイルへのアクセスに関する CLI コマンド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。

表 *33*：*IM and Presence Service* ノードに共通のトレースとトレース 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 Service	`/tomcat/logs/axl/log4j/axl.log`
Cisco Intercluster Sync Agent	`/epas/trace/epassa/log4j/icSyncAgent.log`
Cisco Presence Engine	`/epas/trace/epe/sdi/epe.txt`
Cisco SIP Proxy	`/epas/trace/esp/sdi/esp.txt`
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`

サービス	トレース ログのファイル名
Cisco XCP Client Connection Manager	/epas/trace/xcp/log/client-cm-1*.log
Cisco XCP Config Manager	/epas/trace/xcpconfigmgr/log4j/xcpconfigmgr.log
Cisco XCP Connection Manager	/epas/trace/xcp/log/xmpp-cm-4*.log
Cisco XCP Router	/epas/trace/xcp/log/rtr-jsm-1*.log
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
Cisco XCP XMPP Federation Connection Manager	/epas/trace/xcp/log/xmpp-cm-4*.log
Cluster Manager	/platform/log/clustermgr*
Client Profile Agent（CPA）	/tomcat/logs/epassoap/log4j/EPASSoap*.log
dbmon	/cm/trace/dbl/sdi/dbmon*.txt

IM and Presence Service のログインおよび認証のトレース

IM and Presence Service のユーザが、クライアント ソフトウェアにサインする際に問題に直面している場合、ユーザがプロビジョニングされている IM and Presence Service ノードでトレースを実行できます。次の表に、トレースするサービスのリストを示します。Real-Time Monitoring Tool（RTMT）、または file list および file get などのコマンド ライン インターフェイス（CLI）のコマンドを使用することで、トレース ログ ファイルを表示できます。file get などの CLI コマンドを使用してファイル転送を行う場合は、SFTP サーバのみを使用します。RTMT のインストールおよび使用の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。トレース ログ ファイルへのアクセスに関する CLI コマンド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。

表 *34*：ログインおよび認証問題の調査に使用するトレース

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

サービス	トレース ログのファイル名
Cisco XCP Connection Manager	`/epas/trace/xcp/log/xmpp-cm-4*.log`
Cisco XCP Router	`/epas/trace/xcp/log/rtr-jsm-*.log`
Cisco XCP Authentication Service	`/epas/trace/xcp/logs/auth-svc-1*.log`
Cisco Tomcat Security Logs	`/tomcat/logs/security/log4/security*.log`

可用性、IM、連絡先リスト、およびグループ チャットのトレース

IM and Presence Service の展開の可用性、IM、連絡先リスト、およびグループ チャットのトラブルシューティングにトレースを実行することができます。

次の表に、一般に発生する問題のトレースに推奨されるサービスを示します。

表 *35*：可用性、*IM*、連絡先リスト、およびグループ チャットの問題に推奨されるトレース

問題/ソリューション	サービス
エンド ユーザの連絡先の一部またはすべてに可用性 ステータスがまったく表示されないか、誤った可用性 ステータスが表示されます。 エンド ユーザと連絡先がプロビジョニングされる IM and Presence Service ノードに掲載されているサービスについてのトレースを実行します。	• Cisco XCP Connection Manager • Cisco XCP Router • Cisco Presence Engine
エンド ユーザ自体の話中ステータスまたは会議ステータスなどの可用性 ステータスに問題があります。 エンドユーザがプロビジョニングされる IM and Presence Service ノードに掲載されているサービスについてのトレースを実行します。	• Cisco XCP Connection Manager • Cisco XCP Router • Cisco Presence Engine
エンド ユーザのインスタンス メッセージの送受信に問題があります。 送信者と受信者がプロビジョニングされる IM and Presence Service ノードに掲載されているサービスについてのトレースを実行します。	• Cisco XCP Connection Manager • Cisco XCP Router

問題/ソリューション	サービス
エンドユーザに次の問題のいずれかが発生しています。 • チャット ルームの作成または入室ができない。 • チャット ルーム メッセージがメンバー全員に配信されない。 • チャット ルームの他の問題。 チャット ルームのメンバーがプロビジョニングされる IM and Presence Service ノードに掲載されているサービスについてのトレースを実行します。	• Cisco XCP Connection Manager • Cisco XCP Router • Cisco XCP Text Conferencing Manager
問題が発生しているチャットルームをホストしているノードと、作成者がプロビジョニングされるノードが異なっています。 チャット ルームをホストしているノードを特定するために、初期トレース分析を実行します。次に、チャットルームをホストしている IM and Presence Service ノードで次のサービスのトレースを実行します。	• Cisco XCP Text Conferencing Manager • Cisco XCP Router

トレースが完了すると、リアルタイム監視ツール（RTMT）を使用するか、file list や file get などのコマンドライン インターフェイス（CLI）コマンドを使用してトレース ログ ファイルを表示できます。file get などの CLI コマンドを使用するファイル転送には SFTP サーバのみを使用します。RTMT のインストールおよび使用に関する詳細情報については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。トレース ログ ファイルへのアクセスに関する CLI コマンド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。

- Cisco Presence Engine：`/epas/trace/epe/sdi/epe.txt`
- Cisco XCP Connection Manager：`/epas/trace/xcp/log/xmpp-cm-4*.log`
- Cisco XCP Router：`/epas/trace/xcp/log/rtr-jsm-1*.log`
- Cisco XCP Text Conferencing Manager：`/epas/trace/xcp/log/txt-conf-1*.log`

パーティション化されたドメイン内フェデレーション MOC 連絡先の可用性および IM の問題のトレース

ローカルの IM and Presence Service のユーザが、可用性またはインスタント メッセージを、ドメイン内の Microsoft Office Communicator（MOC）の連絡先とやりとりできない場合、ユーザがプロビジョニングされている IM and Presence Service ノードでトレースを実行できます。次の表に、トレースするサービスのリストを示します。Real-Time Monitoring Tool（RTMT）、または file list お

よび file get などのコマンド ライン インターフェイス（CLI）のコマンドを使用することで、トレース ログ ファイルを表示できます。file get などの CLI コマンドを使用してファイル転送を行う場合は、SFTP サーバのみを使用します。RTMT のインストールおよび使用の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。トレース ログ ファイルへのアクセスに関する CLI コマンド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。

表 *36*：パーティション化されたドメイン内フェデレーション *MOC* 連絡先の可用性および *IM* の問題の調査で使用するトレース

サービス	トレース ログのファイル名
Cisco XCP Router	`/epas/trace/xcp/log/rtr-jsm-1*.log`
Cisco XCP SIP Federation Connection Manager	`/epas/trace/xcp/log/sip-cm-3*.log`
Cisco SIP Proxy	`/epas/trace/esp/sdi/esp.txt`
Cisco Presence Engine	`/epas/trace/epe/sdi/epe.txt`

（注） Cisco SIP Proxy デバッグ ロギングでは、SIP メッセージ交換を確認する必要があります。

XMPP ベースのドメイン間フェデレーション連絡先の可用性および IM の問題のトレース

ローカルの IM and Presence Service のユーザが、可用性 ステータスまたはインスタント メッセージを、ドメイン間フェデレーションの連絡先と交換できない場合、ローカル ユーザがプロビジョニングされている IM and Presence Service ノードでトレースを実行できます。次の表に、トレースするサービスのリストを示します。Real-Time Monitoring Tool（RTMT）、または file list および file get などのコマンド ライン インターフェイス（CLI）のコマンドを使用することで、トレース ログ ファイルを表示できます。file get などの CLI コマンドを使用してファイル転送を行う場合は、SFTP サーバのみを使用します。RTMT のインストールおよび使用の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。トレース ログ ファイルへのアクセスに関する CLI コマンド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。

表 *37*：*XMPP* ベースのドメイン間フェデレーション連絡先に関わる可用性および *IM* 問題の調査で使用するトレース

サービス	トレース ログのファイル名
Cisco XCP Connection Manager	`/epas/trace/xcp/log/xmpp-cm-4*.log`

サービス	トレース ログのファイル名
Cisco XCP Router	`/epas/trace/xcp/log/rtr-jsm-1*.log`
Cisco Presence Engine	`/epas/trace/epe/sdi/epe.txt`
Cisco XCP XMPP Federation Connection Manager 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します。	`/epas/trace/xcp/log/xmpp-cm-4*.log`

SIP ベースのドメイン間フェデレーション連絡先の可用性および IM の問題のトレース

ローカルの IM and Presence Service のユーザが、可用性 ステータスまたはインスタント メッセージを、ドメイン間フェデレーションの連絡先と交換できない場合、ローカル ユーザがプロビジョニングされている IM and Presence Service ノードでトレースを実行できます。次の表に、トレースするサービスのリストを示します。Real-Time Monitoring Tool（RTMT）、または file list および file get などのコマンド ライン インターフェイス（CLI）のコマンドを使用することで、トレース ログ ファイルを表示できます。file get などの CLI コマンドを使用してファイル転送を行う場合は、SFTP サーバのみを使用します。RTMT のインストールおよび使用の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。トレース ログ ファイルへのアクセスに関する CLI コマンド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。

表 *38*：*XMPP* ベースのドメイン間フェデレーション連絡先に関わる可用性および *IM* 問題の調査で使用するトレース

サービス	トレース ログのファイル名
Cisco XCP Connection Manager	`/epas/trace/xcp/log/xmpp-cm-4*.log`
Cisco XCP Router	`/epas/trace/xcp/log/rtr-jsm-1*.log`
Cisco Presence Engine	`/epas/trace/epe/sdi/epe.txt`
Cisco SIP Proxy	`/epas/trace/esp/sdi/esp.txt`
Cisco XCP SIP Federation Connection Manager	`/epas/trace/xcp/log/sip-cm-3*.log`

カレンダー トレース

トレースを実行し、IM and Presence Service 展開についてのカレンダーの問題をトラブルシューティングします。次の表に、トレースするサービスを示します。

トレースの完了後、リアルタイム監視ツール（RTMT）を使用して結果のログ ファイルを表示し、結果の Cisco Presence Engine ログ ファイルで検索をフィルタリングします。“.owa.” および “.ews.”. インスタンスを検索します。また、file list や file get などのコマンド ライン インターフェイス（CLI）コマンドを使用してログ ファイルの結果を表示します。file get などの CLI コマンドを使用するファイル転送には SFTP サーバのみを使用します。RTMT のインストールおよび使用に関する詳細情報については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。トレース ログ ファイルにアクセスする CLI コマンドの使用については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

表 *39*：カレンダーの問題の調査に使用するトレース

サービス	トレース ログのファイル名
Cisco Presence Engine	`/epas/trace/epe/sdi/epe.txt`

クラスタ間同期トレースおよびクラスタ間設定トラブルシュータ

IM and Presence Service ノードが、展開内の別のノードにクラスタ間同期の問題があることを示すアラートを生成する場合、同期していないノードでトレースを実行して、問題を診断することができます。トレースが完了したら、Real-Time Monitoring Tool（RTMT）、または file list および file get などのコマンド ライン インターフェイス（CLI）のコマンドを使用することで、結果のログ ファイルを表示できます。file get などの CLI コマンドを使用してファイルを転送するには、SFTP サーバのみを使用します。RTMT のインストールおよび使用の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。トレース ログ ファイルへのアクセスに関する CLI コマンド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。

また、Cisco Unified CM IM and Presence Administration の GUI でも、同期エラーを確認できます。[診断（Diagnostics）] > [システム トラブルシュータ（System Troubleshooter）] を選択し、[クラスタ間設定トラブルシュータ（Inter-Clustering Troubleshooter）] に移動します。ページの画面スナップをキャプチャできます。

次の表に、クラスタ間同期問題をトレースするサービスのリストを示します。クラスタ間同期の問題がある各 IM and Presence Service ノードで、リストされたサービスのトレースを実行します。

表 *40*：クラスタ間同期問題の調査でノード間で使用するトレース

サービス	トレース ログのファイル名
Cisco Intercluster Sync Agent	`/epas/trace/epassa/log4j/icSyncAgent.log`

サービス	トレース ログのファイル名
Cisco AXL Web Service	`/tomcat/logs/axl/log4j/axl.log`
Cisco Tomcat Security Log	`/tomcat/logs/security/log4/security*.log`
Cisco Syslog Agent	`/cm/trace/syslogmib/sdi/syslogmib.txt`

SIP フェデレーション トレース

トレースを実行することで、IM and Presence サービスの展開における SIP フェデレーション問題を修復できます。次の表に、トレースするサービスのリストを示します。

トレースが完了したら、Real-Time Monitoring Tool（RTMT）、または file list や file get などの Command Line Interface（CLI）コマンドを使用して結果のログ ファイルを表示できます。file get などの CLI コマンドを使用してファイルを転送するには、SFTP サーバのみを使用します。RTMT のインストールおよび使用の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。トレース ログ ファイルにアクセスする CLI コマンドの使用に関する詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

表 *41*：ログインおよび認証問題の調査に使用するトレース

サービス	トレース ログのファイル名
Cisco SIP Proxy	`/epas/trace/esp/sdi/esp.txt`
Cisco XCP Router	`/epas/trace/xcp/log/rtr-jsm-*.log`
Cisco XCP SIP Federation Connection Manager	`/epas/trace/xcp/log/sip-cm-3*.log`

XMPP フェデレーション トレース

トレースを実行することで、IM and Presence サービス展開の XMPP フェデレーション問題を修復できます。次の表に、トレースするサービスのリストを示します。

トレースが完了したら、Real-Time Monitoring Tool（RTMT）、または file list や file get などの Command Line Interface（CLI）コマンドを使用して結果のログ ファイルを表示できます。file get などの CLI コマンドを使用してファイルを転送するには、SFTP サーバのみを使用します。RTMT のインストールおよび使用の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。トレース ログ ファイルにアクセスする CLI コマンドの使用に関する詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

表 *42* : ***XMPP*** フェデレーション問題を調査するために使用されるトレース

サービス	トレース ログのファイル名
Cisco XCP Router	`/epas/trace/xcp/log/rtr-jsm-*.log`
Cisco XCP XMPP Federation Connection Manager	`/epas/trace/xcp/log/xmpp-cm-4*.log`

高 CPU と低 VM のアラートのトラブルシューティング

IM and Presence Service ノードが高 CPU または低 VM の可用性 アラートを生成している場合、コマンド ライン インターフェイス（CLI）を使用することで、原因の特定に役立つ情報をノードから収集できます。また、関連するサービスのトレースをノードで実行することもでき、Real-Time Monitoring Tool（RTMT）を使用して、結果のログ ファイルを表示することもできます。RTMT のインストールおよび使用の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。CLI コマンドの使用については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

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。IM and Presence Service は、アプリケーション ログにシステムエラーを書き込みます。そのログを表示するには、SysLog ビューアを RTMT で使用します。サービスの syslog アラームの設定の詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。SysLog ビューアを使用したアラーム情報の表示については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

表 *43* : 高 ***CPU*** と低 ***VM*** のアラートの調査で使用する ***CLI*** コマンド

ソリューション	**CLI** コマンド

CLI を使用して、ノードで次の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`

CLI を使用して、ノードのすべての RIS（Real-time Information Service）のパフォーマンス ログを収集します。file get を使用してファイル転送を行う場合は、SFTP サーバのみを使用します。	`file get activelog cm/log/ris/csv`

次の表は、高 CPU と低 VM のアラートを調査するために、IM and Presence Service ノードでトレースを実行するタイミングを選択するための、サービスのリストです。高 CPU または低 VM のア

ラートを生成している IM and Presence Service ノードで、リストされたサービスのトレースを実行します。

表 *44*：高 *CPU* と低 *VM* のアラートの調査で使用するトレース

サービス	トレース ログのファイル名
Cisco XCP Router	`/epas/trace/xcp/log/rtr-jsm-1*.log`
Cisco XCP SIP Federation Connection Manager	`/epas/trace/xcp/log/sip-cm-3*.log`
Cisco SIP Proxy	`/epas/trace/esp/sdi/esp.txt`
Cisco Presence Engine	`/epas/trace/epe/sdi/epe.txt`
Cisco Tomcat Security Log	`/tomcat/logs/security/log4/security*.log`
Cisco Syslog Agent	`/cm/trace/syslogmib/sdi/syslogmib.txt`

付 録 A

高可用性クライアントログインプロファイル

高可用性 ログイン プロファイル

高可用性 ログイン プロファイルに関する重要事項

- この項の高可用性 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。
- 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 サイズおよび各高可用性展開タイプ（アクティブ/アクティブまたはアクティブ/スタンバイ）用に高可用性 ログイン プロファイルを提供します。
- 高可用性 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、高可用性 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。

高可用性 ログイン プロファイル テーブルの使用

高可用性 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

ステップ 1 および仮想ハードウェア設定および高可用性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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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 のフル米国プロファイル - IM only 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	312

（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 5,000 のフル米国プロファイル - IM only アクティブ/アクティブ展開

IM-only 展開で、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
[5000]	120	923

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 *45*：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	320
250（デフォルト）	120	620
IM のみ		
[500]	120	1120

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 *46*：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	253
250（デフォルト）	120	453
[500]	120	787
IM のみ		
750	120	1120
[1000]	120	1453

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 *47*：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	220
250	120	370
500（デフォルト）	120	620
IM のみ		
750	120	870
[1000]	120	1120

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 *48*：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	187
250	120	287
500（デフォルト）	120	453
750	120	620
[1000]	120	787
IM のみ		
1250	120	953
1500	120	1120
1750	120	1287
2000	120	1453

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 *49*：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	220

アクティブ ユーザの予想数	再試行下限値	再試行上限値
500（デフォルト）	120	620
[1000]	120	1120

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 *50*：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	187
250	120	287
500（デフォルト）	120	453
750	120	620
[1000]	120	787
1250	120	953
1500	120	1120
1750	120	1287
2000	120	1453

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 *51*：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	170
[500]	120	370
[1000]	120	620
1500	120	870
2000	120	1120
2500（デフォルト）	120	1370
IM のみ		
3000	120	1620
3500	120	1870
4000	120	2120
4500	120	2370
[5000]	120	2620
6000	120	3120
6250	120	3245

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

表 *52*：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	153
[500]	120	287
[1000]	120	453
1500	120	620
2000	120	787
2500（デフォルト）	120	953
3000	120	1120
3500	120	1287
4000	120	1453
4500	120	1620
[5000]	120	1787
IM のみ		
6000	120	2120
7000	120	2453
8000	120	2787
9000	120	3120
10000	120	3453
11000	120	3787
12000	120	4120

アクティブ ユーザの予想数	再試行下限値	再試行上限値
12500	120	4287

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

表 *53*：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		
100	120	153
[500]	120	287
[1000]	120	453
1500	120	620
2000	120	787
2500	120	953
3000	120	1120
3500	120	1287
4000	120	1453
4500	120	1620
5000（デフォルト）	120	1787
6000	120	2120
7000	120	2453
7500	120	2620
IM のみ		
8000	120	2787

アクティブ ユーザの予想数	再試行下限値	再試行上限値
9000	120	3120
10000	120	3453
11000	120	3787
12000	120	4120
12500	120	4287

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

表 *54*：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	140
[500]	120	220
[1000]	120	320
1500	120	420
2000	120	520
2500	120	620
3000	120	720
3500	120	820
4000	120	920
4500	120	1020
5000（デフォルト）	120	1120

アクティブ ユーザの予想数	再試行下限値	再試行上限値
6000	120	1320
7000	120	1520
8000	120	1720
9000	120	1920
10000	120	2120
11000	120	2320
12000	120	2520
13000	120	2720
14000	120	2920
15000	120	3120
IM のみ		
16000	120	3320
17000	120	3520
18000	120	3720
19000	120	3920
20000	120	4120
21000	120	4320
22000	120	4520
23000	120	4720
24000	120	4920
25000	120	5120

付 録 B

XMPP 標準への準拠

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)