Cisco Unified Communications Manager の IM and Presence サービスのパーティションイントラドメインフェデレーション、リリース 9.0(1)

初版：2012 年 07 月 18 日

最終更新：2012 年 07 月 18 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 1 章

統合の概要

パーティション イントラドメイン フェデレーション

IM およびアベイラビリティ プラットフォームとして IM and Presence を選択する企業はますます増えています。 これらの企業ではすでに、Microsoft Office Communications Server（OCS）または Microsoft Live Communications Server（LCS）が導入されており、ユーザを Microsoft Office Communicator から IM and Presence 対応クライアントに移行させたいと考えています。 遷移中、IM and Presence 対応クライアントに移行するこれらのユーザが、Microsoft Office Communicator を使用しているユーザとプレゼンス情報およびインスタント メッセージを引き続き共有できることが大切です。 対応している IM and Presence クライアントの詳細については、「“ソフトウェア要件”」の項を参照してください。

パーティション イントラドメイン フェデレーションでは、同一企業ドメイン内の IM and Presence クライアント ユーザと Microsoft Office Communicator ユーザが、プレゼンス アベイラビリティと Instant Messaging（IM; インスタント メッセージ）を交換できます。

この統合では、IM and Presence で設定され、IM and Presence 対応クライアントをデスクトップ クライアントとして使用するか、OCS または LCS で有効化され、Microsoft Office Communicator をデスクトップ クライアントとして使用する、企業ドメイン内のユーザがサポートされます。

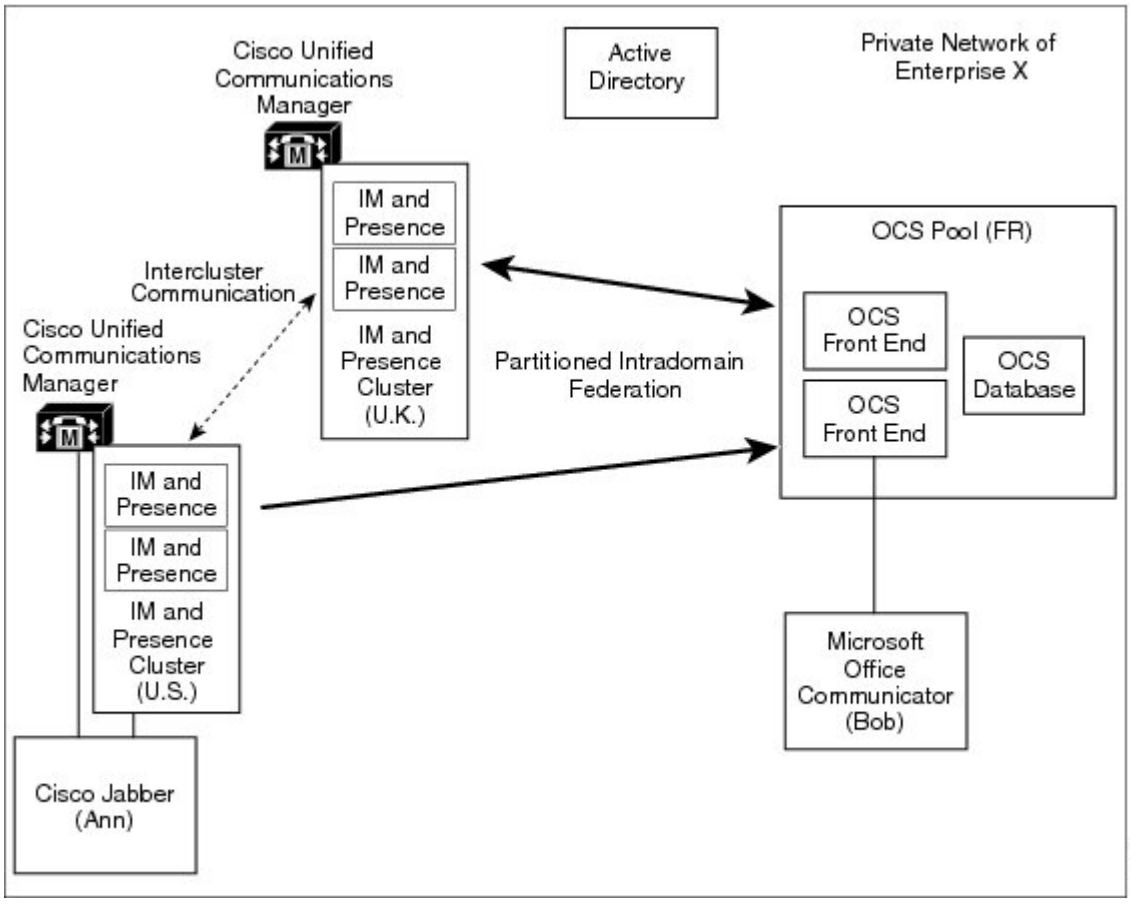
（注） この統合では、IM and Presence 対応クライアントと Microsoft Office Communicator 両方を持つユーザはサポートされていません。

IM and Presence リリース 9.0 は、スタンドアロン Session Initiation Protocol（SIP RFC 3261）を使用して、次の LCS/OCS プラットフォームのパーティション イントラドメイン フェデレーションを提供します。

- Microsoft Live Communications Server 2005 Standard Edition および Enterprise Edition
- Microsoft Office Communications Server 2007 R2 Standard Edition および Enterprise Edition

次の図は、IM and Presence と LCS/OCS を同じドメイン内に導入した例の概要を示します。

図 *1*：統合の概要



（注） このマニュアルで LCS/OCS と言う用語はサポート対象のすべての LCS および OCS プラットフォームのタイプを示します。 あるプラットフォームに固有の詳細がある場合、その LCS または OCS プラットフォームについて具体的に示します。

関連トピック

ソフトウェア要件, （22 ページ）

アベイラビリティ

ここでは、次の機能について説明します。

アベイラビリティの登録およびポリシー

ここでは、次のコール フローについて説明します。

IM and Presence へのユーザ登録

Microsoft Office Communicator ユーザが IM and Presence クライアント ユーザのプレゼンスを表示する場合、SIP SUBSCRIBE 要求が LCS/OCS から IM and Presence へルーティングされます。 IM and Presence は着信登録を承認し、それを保留中にします。 プライベート ポリシーがこの着信登録要求に適用されます。

（注） パーティション イントラドメイン フェデレーション展開で Microsoft Office Communicator ユーザからの登録に適用されたプライバシー ポリシーは、IM and Presence クライアント ユーザからの登録に適用されるプライバシー ポリシーと同じです。

IM and Presence は、自動認証が有効になっているかどうか、または IM and Presence クライアント ユーザが Microsoft Office Communicator ユーザのプレゼンス登録を以前にブロックしたまたは許可したかどうか確認します。 いずれかが true の場合、IM and Presence は、登録要求のポリシー判断を自動で処理します。 それ以外の場合は、IM and Presence クライアント ユーザは、新規登録に関する警告を受信します。

登録が拒否される場合、Polite Blocking が実装されています。 つまり、ユーザのプレゼンス状態が Microsoft Office Communicator ユーザにオフラインとして表示されています。 登録が認証されると、IM and Presence はプレゼンス アップデートを Microsoft Office Communicator ユーザに送信し、IM and Presence クライアント ユーザには Microsoft Office Communicator ユーザをその参加者に追加するオプションがあります。

Microsoft Office Communicator へのユーザ登録

IM and Presence クライアント ユーザが Microsoft Office Communicator ユーザのプレゼンスを表示する場合、SIP SUBSCRIBE 要求が IM and Presence から LCS/OCS へルーティングされます。 LCS/OCS は着信登録を承認します。 ポリシーがこの着信登録要求に適用されます。

Microsoft Office Communicator ユーザが以前にこのユーザからの登録を承認している場合、その登録は自動的に承認され、Microsoft Office Communicator ユーザにより適用されたポリシー レベルにしたがってプレゼンスが IM and Presence クライアント ユーザに返されます。 そうでない場合、Microsoft Office Communicator ユーザは新規登録についての警告を受信します。 Microsoft Office Communicator ユーザは IM and Presence クライアント ユーザを承認またはブロックできます。

（注） Microsoft Office Communicator は 1 時間 45 分ごとに更新サブスクライブを行います。 したがって、IM and Presence サーバが再起動する場合、Microsoft Office Communicator ユーザに IM and Presence 連絡先のプレゼンス状態がない時間は最長で約 2 時間になります。

（注） LCS/OCS が再起動する場合、IM and Presence クライアントに Microsoft Office Communicator 連絡先のプレゼンス状態がない時間は最長で約 2 時間になります。

アベイラビリティ マッピング状態

次の表は Microsoft Office Communicator から次の IM and Presence 対応クライアントへのアベイラビリティ マッピング状態を示します。

- Cisco Jabber リリース 8.x
- Cisco Jabber for Mac
- サードパーティ製の XMPP クライアント

表 *1*：*Microsoft Office Communicator* からのアベイラビリティ マッピング状態

Microsoft Office Communicator 設定	Cisco Jabber 8.x 設定	Cisco Jabber for Mac 設定	サードパーティ製の XMPP クライアント設定
利用可能	利用可能	利用可能	利用可能

Microsoft Office Communicator 設定	Cisco Jabber 8.x 設定	Cisco Jabber for Mac 設定	サードパーティ製の XMPP クライアント設定
退席中	退席中	退席中	退席中
すぐに戻ります	退席中	退席中	退席中
ビジー（Busy）	ビジー（Busy）	ビジー（Busy）	ビジー（Busy）
サイレント	ビジー（Busy）	ビジー（Busy）	ビジー（Busy）
オフライン表示	オフライン	オフライン	オフライン
オフライン	オフライン	オフライン	オフライン

次の表は Cisco Jabber リリース 8.x から Microsoft Office Communicator へのアベイラビリティ マッピング状態を示します。

表 *2*：*Cisco Jabber* リリース *8.x* から *Microsoft Office Communicator* へのアベイラビリティ マッピング状態

Cisco Unified Jabber リリース 8.x 設定	Microsoft Office Communicator 設定
利用可能	利用可能
ビジー（Busy）	ビジー（Busy）
電話中（On the Phone）	ビジー（Busy）
会議（Meeting）	ビジー（Busy）
退席中	退席中
サイレント	ビジー（Busy）
オフライン	オフライン
オフライン：電話中	オフライン
オフライン：会議	オフライン
オフライン：外出中	オフライン

次の表は Cisco Jabber for Mac から Microsoft Office Communicator へのアベイラビリティ マッピング状態を示します。

表 *3*：*Cisco Jabber for Mac* から *Microsoft Office Communicator* へのアベイラビリティ マッピング状態

Cisco Jabber for Mac 設定	**Microsoft Office Communicator 設定**
利用可能	利用可能
退席中	退席中
サイレント	ビジー（Busy）
不在	オフライン
オフライン	オフライン

次の表はサードパーティ製の XMPP クライアントから Microsoft Office Communicator へのアベイラビリティ マッピング状態を示します。

表 *4*：サードパーティ製の *XMPP* クライアントから *Microsoft Office Communicator* へのアベイラビリティ マッピング状態

サードパーティ製の XMPP 設定	**Microsoft Office Communicator 設定**
利用可能	利用可能
退席中	退席中
退席中（延長）	退席中
サイレント	ビジー（Busy）
オフライン	オフライン

インスタント メッセージ

パーティション イントラドメイン フェデレーションでは、IM and Presence クライアント ユーザと Microsoft Office Communicator ユーザ間のポイントツーポイント IM をサポートしています。 次のような IM 機能がサポートされています。

- プレーン テキスト IM フォーマット

- 入力指示
- 基本顔文字

SIP Session Mode IM を使用して、IM and Presence と LCS/OCS 間でメッセージおよび入力指示を転送します。

IM and Presence クライアント ユーザが IM を Microsoft Office Communicator ユーザに送信すると、これらの 2 人のユーザ間で既存の IM セッションが確立されていない場合、IM and Presence は SIP INVITE メッセージを LCS/OCS に送信して、新しいセッションを確立します。 このセッションは、これら 2 人のユーザいずれかからの以降の SIP MESSAGE または SIP INFO（入力指示）トラフィックに使用します。

（注） IM and Presence クライアント ユーザおよびサードパーティ製 XMPP クライアント ユーザは、アベイラビリティがなくても、Microsoft Office Communicator ユーザと IM 会話を開始できます。

Microsoft Office Communicator ユーザが IM を IM and Presence クライアント ユーザに送信すると、これらの 2 人のユーザ間で既存の IM セッションが確立されていない場合、Microsoft Office Communicator は SIP INVITE メッセージを IM and Presence に送信します。 このセッションは、これら 2 人のユーザいずれかからの以降の SIP MESSAGE または SIP INFO（入力指示）トラフィックに使用します。

（注） LCS/OCS グループ チャット機能独自の特性により、パーティション イントラドメイン フェデレーションでは、IM and Presence クライアント ユーザと Microsoft Office Communicator ユーザ間のグループ チャットはサポートされていません。

要求のルーティング

ここでは、IM and Presence から LCS/OCS、また LCS/OCS から IM and Presence への要求のルーティングについて説明します。

- IM and Presence から LCS/OCS への要求のルーティング, （7 ページ）
- LCS/OCS から IM and Presence への要求のルーティング, （10 ページ）

IM and Presence から LCS/OCS への要求のルーティング

IM and Presence から LCS/OCS への基本的な接続を有効にするには、IM and Presence ドメインに対して IM and Presence で SIP スタティック ルートを設定する必要があります。 これらのスタティック ルートは LCS/OCS サーバまたはフロントエンド ロードバランサ（Enterprise Edition では LCS/OC のみ）の IP アドレスをポイントし、受信者が IM and Presence ユーザでない場合に、IM and Presence が same-domain 要求を LCS/OCS にルーティングできるようにします。 トランスポート層セキュリ

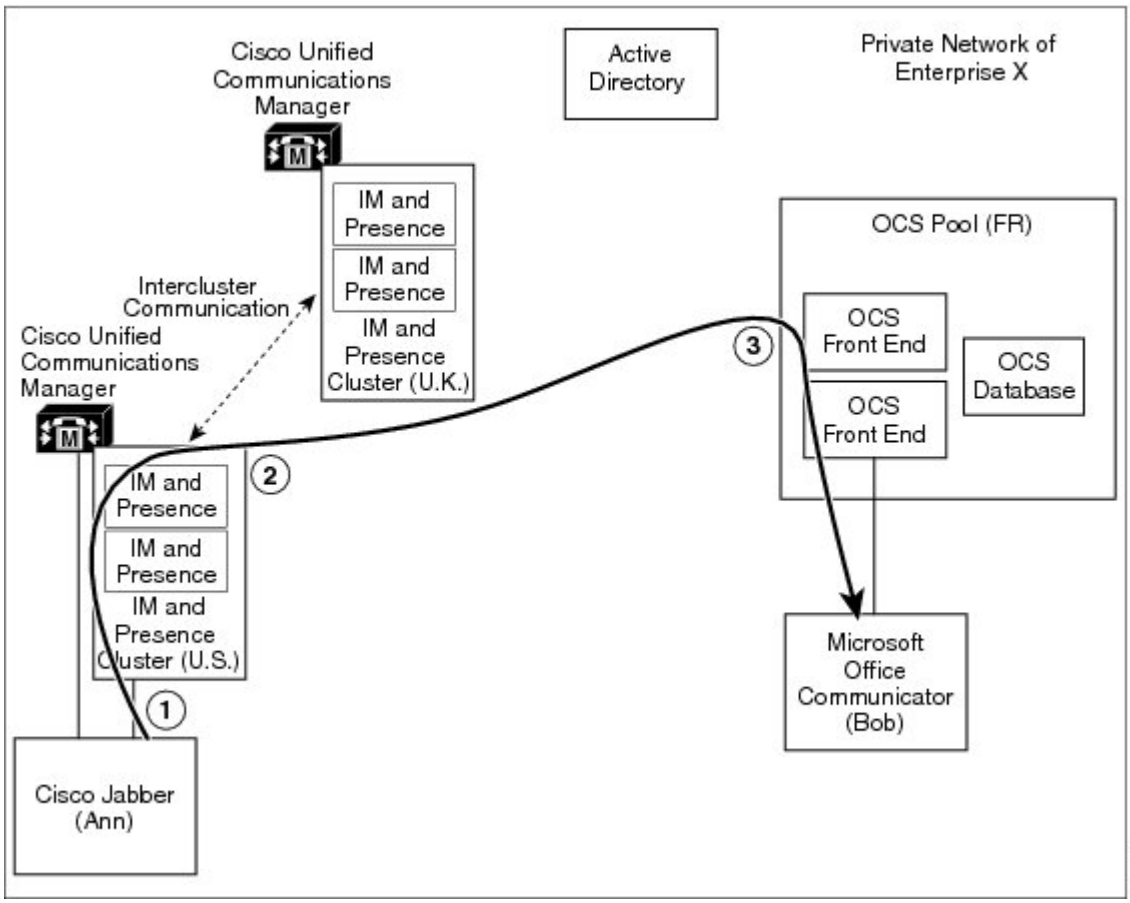
ティ（TLS）暗号化をこれらのスタティック ルートで有効にできます。 また IM and Presence から LCS/OCS への基本的な接続をサポートするには、着信アクセス コントロール リスト（ACL）のエントリを設定し、認証がなくても LCS/OCS サーバが IM and Presence サーバにアクセスできるようにする必要があります。

この基本的な接続に重なるように、パーティションイントラドメインフェデレーションでは、IM and Presence から LCS/OCS への要求のルーティングに対して、基本ルーティングおよび高度なルーティングという 2 種類のモードを提供しています。

基本的なルーティングは、パーティションイントラドメインフェデレーションのデフォルト ルーティング モードです。 基本的なルーティングが有効な場合、要求の受信者が IM and Presence ドメイン内に存在しているものの、ライセンスされた IM and Presence ユーザでない場合に、IM and Presence は要求を LCS/OCS にルーティングします。

次の図は、基本的なルーティングが設定されている場合の IM and Presence から LCS/OCS へのルーティング要求のシーケンスを示しています。

図 *2*：*IM and Presence* から *LCS/OCS* への要求のルーティング



（注）
- IM and Presence または LCS/OCS のいずれかでプロビジョニングされていない受信者について、LCS/OCS に転送される該当するあらゆる要求は、今度は LCS/OCS により IM and Presence へ返されます。
- IM and Presence は、この方法で LCS/OCS からループバックする要求を拒否する組み込みループ検出を備えています。

1	Cisco Jabber 8.x ユーザの Ann は、Microsoft Office Communicator ユーザである Bob に要求を送信します。
2	Bob はローカル ドメイン内にいるものの、ライセンスされた IM and Presence クライアント ユーザではないため、IM and Presence は要求を変換し、それを LCS/OCS にルーティングします。
3	LCS/OCS サーバは要求を Bob の Microsoft Office Communicator クライアントに転送します。

Cisco Unified Communications Manager がそのユーザを、LCS/OCS で使用される同じ Active Directory から同期している場合のみ、高度なルーティングを設定します。 Active Directory から同期されたユーザのリストには、すべての Microsoft Office Communicator ユーザが記載されている必要があります。 高度なルーティングが有効な場合、次に示す条件を両方とも満たしている場合に IM and Presence は要求を LCS/OCS にルーティングします。

- 要求の受信者は IM and Presence ドメイン内に存在するが、ライセンスされた IM and Presence ユーザではない。

  かつ

- 要求の受信者の有効な Microsoft Office Communicator SIP アドレスが IM and Presence データベースに保存されている。

（注）
- 拡張ルーティングは、シングル クラスタの IM and Presence 配置でのみサポートされています。
- 高度なルーティングにより IM and Presence データベースに多数のプロビジョニングされていない、または不明な連絡先がある展開で、IM and Presence および LCS/OCS 間のトラフィック量が少なくなります。
- ただし、高度なルーティングは IM and Presence クラスタそれぞれにストレージ オーバーヘッドを追加します。高度なルーティングのロジックを適用できるためには、すべての Microsoft Office Communicator ユーザをクラスタごとに保存する必要があるためです。

LCS/OCS から IM and Presence への要求のルーティング

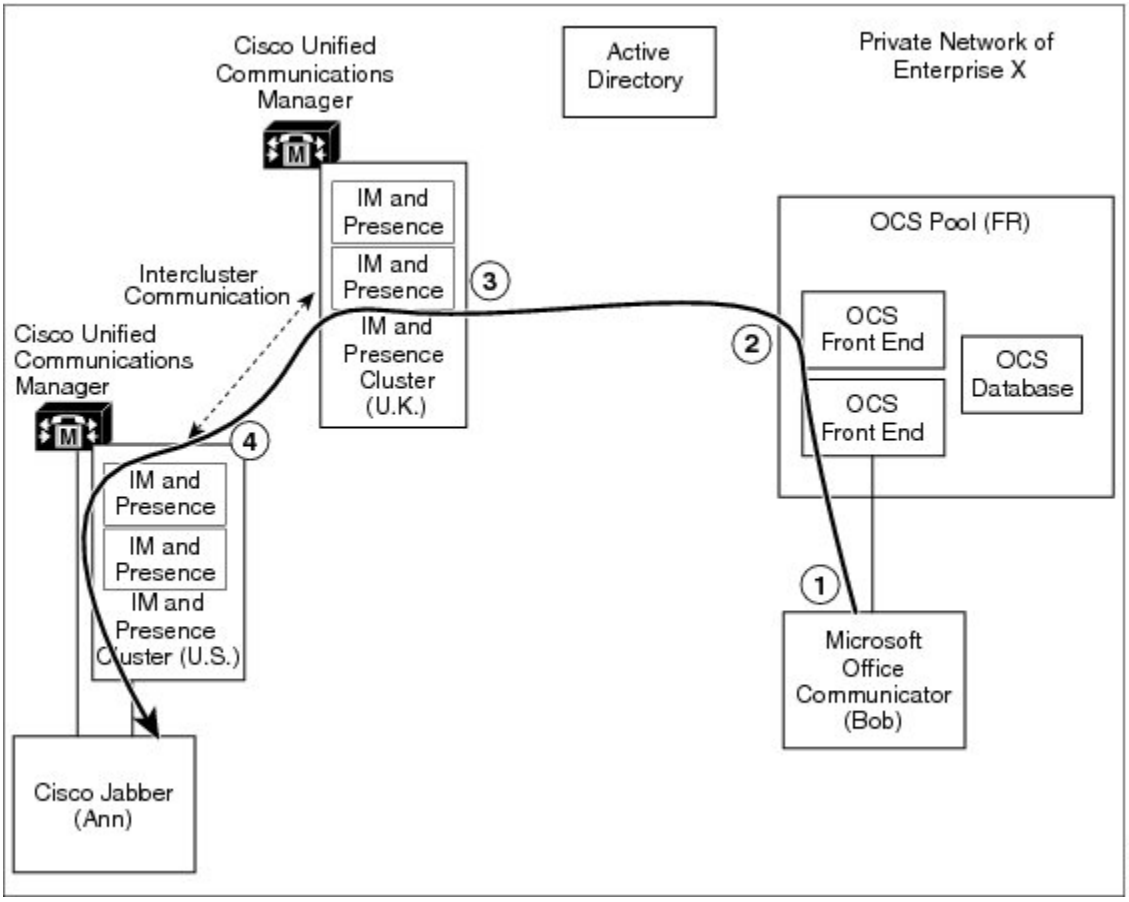
LCS/OCS から IM and Presence への基本的な接続を有効にするには、IM and Presence ドメインに対して LCS/OCS で SIP スタティック ルートを設定する必要があります。 これらのスタティック ルートは IM and Presence サーバの IP アドレスおよびポートをポイントします。このサーバはルーティング IM and Presence サーバとして指定されています。 これらのルートにより、受信者が LCS/OCS ユーザでない場合に、LCS/OCS は same-domain 要求を IM and Presence にルーティングできるようになります。 TLS 暗号化をこれらのスタティック ルートで有効にできます。

IM and Presence から SIP 要求を承認するための認証要求が LCS/OCS に出されないようにするため、LCS/OCS の IM and Presence サーバごとにホスト認証エントリも設定する必要があります。

すでに説明したように、スタティック ルート設定に重なるように、パーティション イントラドメイン フェデレーション展開では、LCS/OCS にはルーティング モードは 1 つしかありません。 要求の受信者が LCS/OCS 管理プレゼンス ドメインのいずれかに存在しているものの、Microsoft Office Communicator ユーザでない場合に、LCS/OCS は要求を IM and Presence にルーティングします。

次の図は、LCS/OCS から IM and Presence へのルーティング要求のシーケンスを示しています。

図 *3*：*LCS/OCS* から *IM and Presence* への要求のルーティング



（注） IM and Presence またはLCS/OCS のいずれかでプロビジョニングされていない受信者について、LCS/OCS から IM and Presence に転送される該当するあらゆる要求は、IM and Presence により拒否されます。

1	Microsoft Office Communicator ユーザの Bob は、Cisco Jabber 8.x ユーザである Ann に要求を送信します。	3	IM and Presence は要求を承認し、Ann の自宅の IM and Presence サーバに転送します。
2	Ann はローカル ドメイン内にいるものの、Microsoft Office Communicator ユーザではないため、LCS/OCS は要求を IM and Presence にルーティングします。	4	IM and Presence は要求を変換し、Ann の Cisco Jabber クライアントに転送します。

クラスタ間展開とマルチノード展開

クラスタ間およびマルチノード クラスタ IM and Presence 展開では、アベイラビリティの登録または IM 会話を行う場合、LCS/OCS サーバはすべての SIP メッセージを、ルーティング目的で指定された IM and Presence サーバにルーティングします。 IM and Presence ルーティング サーバで受信ユーザがホストされていない場合、メッセージは展開内の適切な IM and Presence サーバにルーティングされます。 システムは、ルーティング IM and Presence サーバを介して、この要求に関連付けられたすべての応答をルーティングします。

アベイラビリティの登録または IM 会話を行う場合、どの IM and Presence サーバも SIP メッセージを直接 LCS/OCS サーバに送信できます。 LCS/OCS がこれらのメッセージに返信すると、返信は、メッセージを開始した IM and Presence サーバに直接送信されます。

ドメイン間フェデレーション

IM and Presence では、ドメイン間フェデレーションがサポートされています。 この機能は、IM and Presence がパーティション イントラドメイン フェデレーションに設定されている場合も使用できます。 ただし、IM and Presence で設定されているどのドメイン間フェデレーションも IM and Presence クライアント ユーザにのみ使用できます。

LCS/OCS 展開がすでに Access Edge/Access Proxy サーバを介して SIP ドメイン間フェデレーションに設定されている場合、Microsoft Office Communicator ユーザはこのフェデレーション機能を継続して使用できます。 IM and Presence クライアント ユーザがそうした既存のフェデレーション機能を活用できるように、IM and Presence および LCS/OCS を設定することもできます。

（注）

- IM and Presence と LCS/OCS 両方を設定して、同じリモート ドメインで直接フェデレーションすることはサポートされていません。
- IM and Presence ドメイン間フェデレーションの詳細については、マニュアル『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

（注）

関連トピック

IM and Presence のドメイン内 LCS/OCS のドメイン間フェデレーション機能との統合, （101 ページ）
『Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager』

ドメイン内フェデレーションのハイ アベイラビリティ

パーティション イントラドメイン フェデレーションは、IM and Presence と LCS/OCS 間の要求のルーティングについて、ハイ アベイラビリティをサポートします。

IM and Presence から LCS/OCS への要求のルーティングのハイ アベイラビリティ

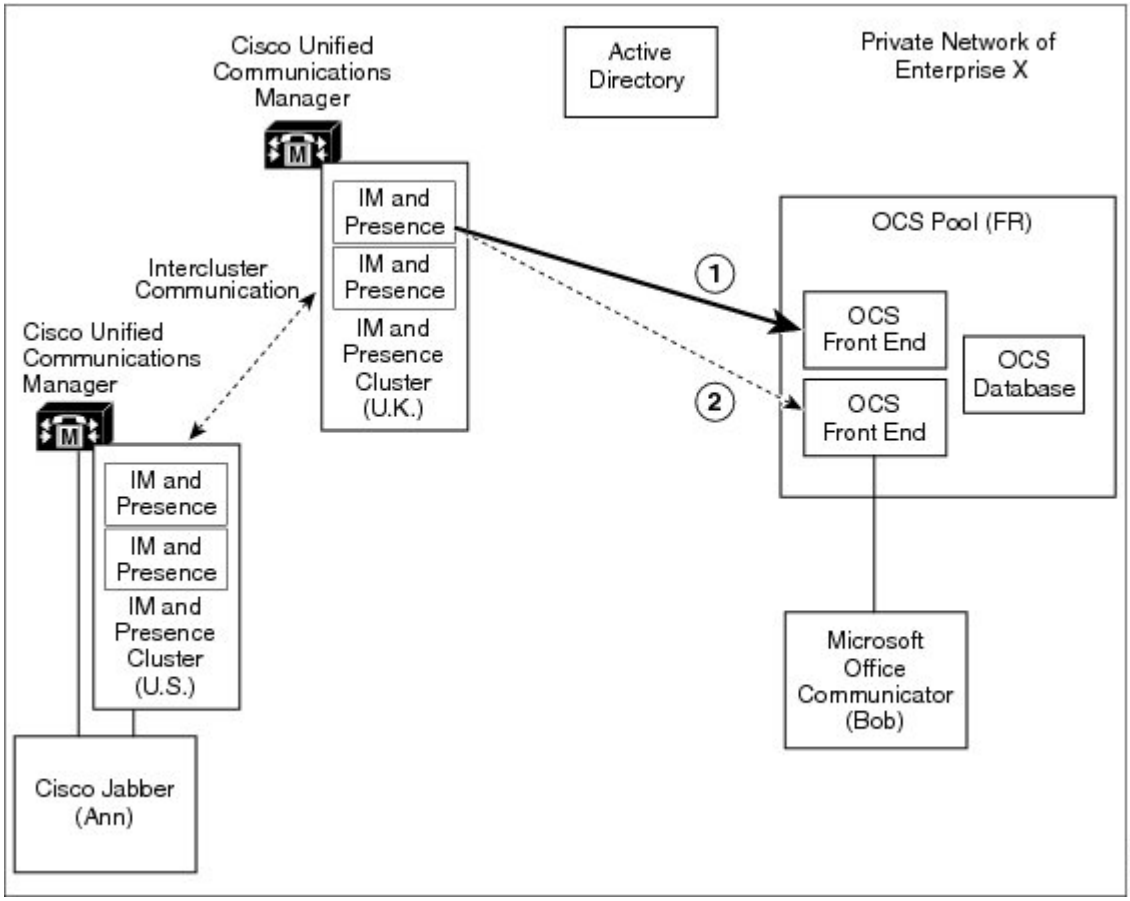
前述したように、SIP スタティック ルートを IM and Presence で設定して、IM and Presence および LCS/OCS 間のドメイン内フェデレーションの基本的な接続を有効にする必要があります。

LCS/OCS との統合においてハイ アベイラビリティを実現するため、IM and Presence でアドレス パターンごとに複数の SIP スタティック ルートを設定できます。

必要に応じて、これらのスタティック ルートにプライオリティ値を割り当て、プライマリとバックアップのスタティック ルートを定義できます。プライオリティが最も高いルートが最初に試行

されます。これらのルートが使用できない場合、次の図に示すように、要求はバックアップルートを使用して再送信されます。

図 *4* : *IM and Presence* から *LCS/OCS* への要求のルーティングのハイ アベイラビリティ

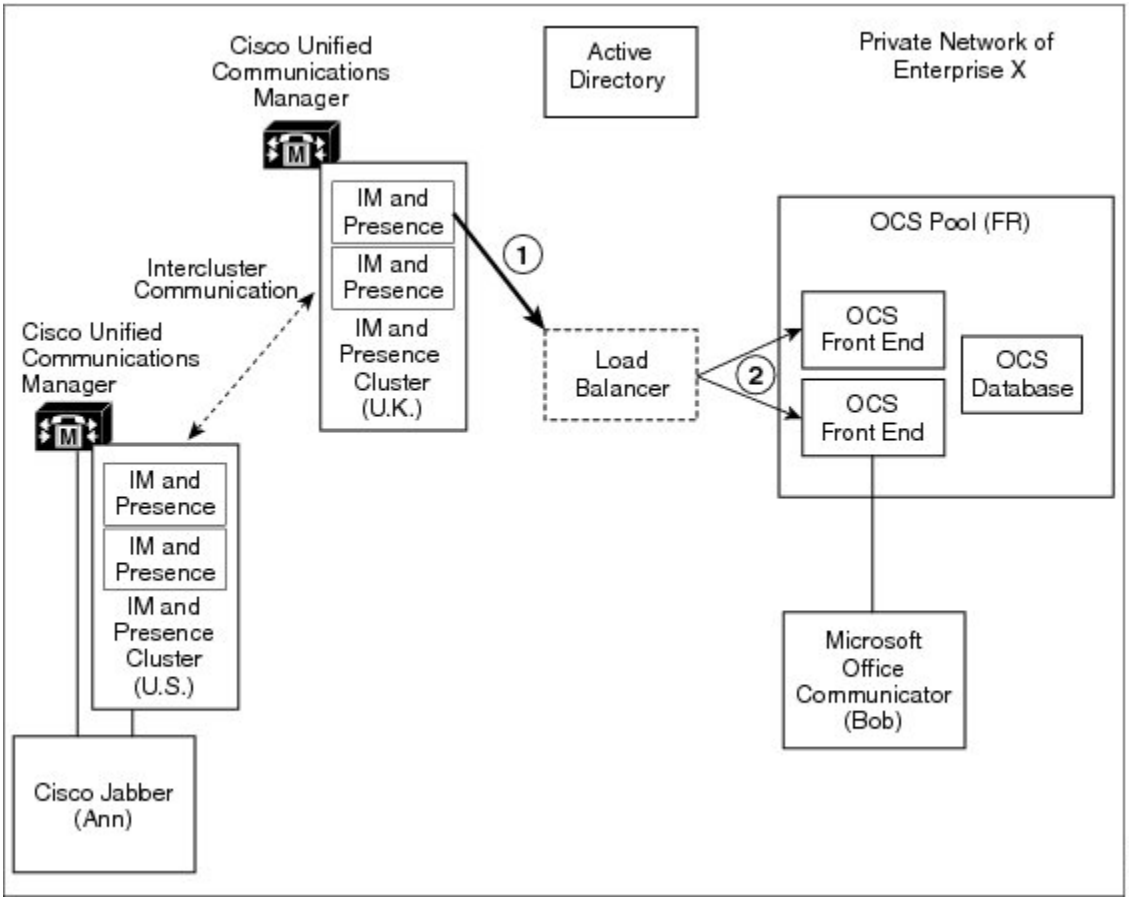


1	LCS/OCS にルーティングする場合、IM and Presence はプライオリティが最も高いスタティック ルートを見つけ、要求をそのルートに設定されたネクスト ホップ アドレスに送信しようとします。	2	そのネクスト ホップが使用できない場合、IM and Presence はプライオリティが次に高いスタティック ルートにフォールバックし、要求を関連するネクスト ホップ アドレスに送信しようとします。

Enterprise Edition LCS/OCS の場合、フロントエンド ロード バランサを展開できます。 その場合、SIP スタティック ルートを IM and Presence に設定して、LCS/OCS フロントエンド ロード バラン

サの IP アドレスをポイントできます。 フロントエンド ロード バランサは、次の図に示すようにその関連付けられた LCS/OCS プール内でハイ アベイラビリティを実現します。

図 *5*：ロード バランサによる *IM and Presence* から *LCS/OCS* への要求のルーティングのハイ アベイラビリティ



1	LCS/OCS にルーティングする場合、IM and Presence は OCS フロントエンド ロード バランサをポイントするスタティック ルートを見つけます。	2	LCS/OCS フロントエンド ロード バランサは、プール内のアクティブなフロントエンド サーバのいずれかにルーティングします。

IM and Presence は、LCS/OCS フロントエンド ロード バランサとして Cisco Application Control Engine（ACE）を使用してテストされています。 ACE の代わりに他のロードバランサを使用できます。認定されたロード バランサのリストについては次の URL を参照してください。http://technet.microsoft.com/en-us/office/ocs/cc843611 ただし、それらのロード バランサを導入し、正しく管理するのはお客様の責任です。

（注） シスコでは、ACE 以外のロード バランサをポイントするスタティック ルートの設定はサポートしていません。

ACEが設定されたフロントエンドのロードバランサでないような導入環境では、フロントエンドロードバランサをバイパスするためのスタティック ルートを設定することをお勧めします。

LCS/OCS から IM and Presence への要求のルーティングのハイ アベイラビリティ

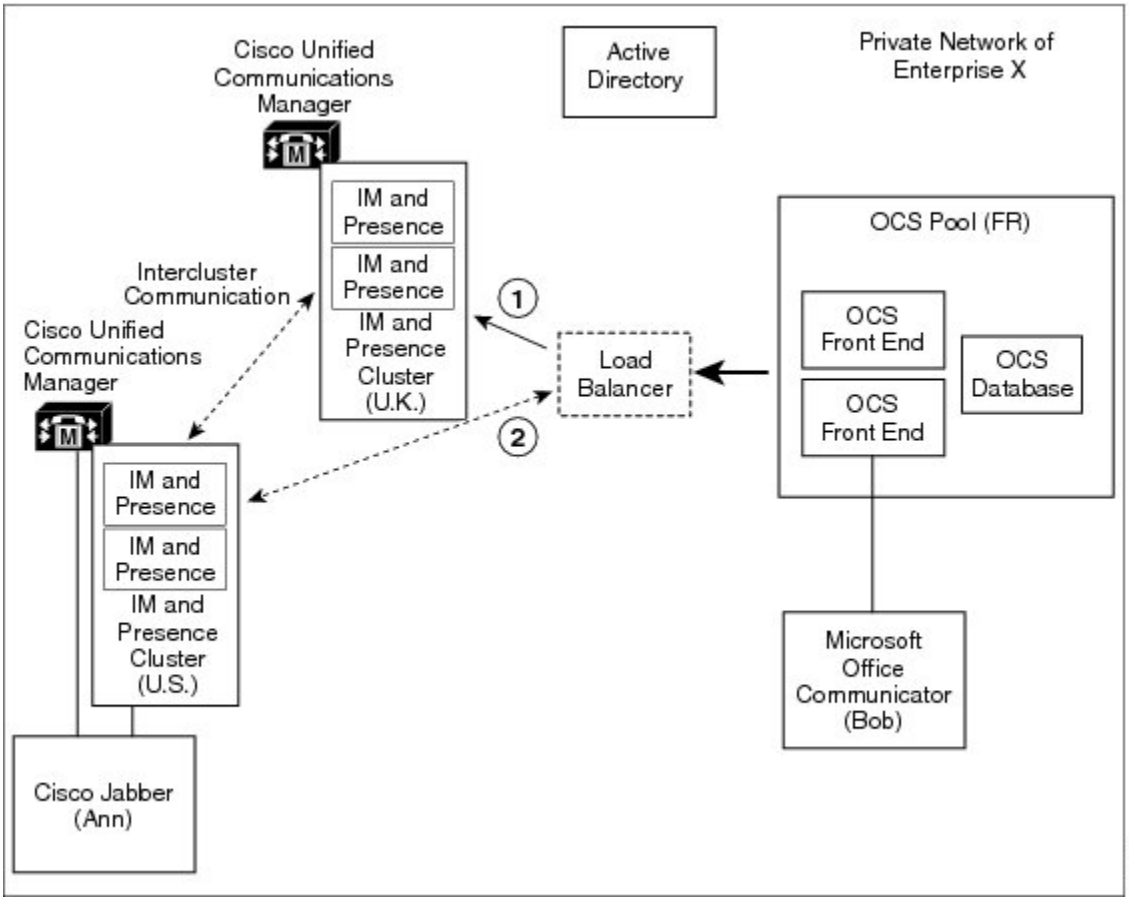
SIP スタティック ルートを LCS/OCS で設定して、LCS/OCS および IM and Presence 間のドメイン内フェデレーションの基本的な接続を有効にする必要があります。

ただし、LCS/OCS はドメインごとに 1 つの SIP スタティック ルートのみ設定できます。つまり、スタティック ルートは単一の IM and Presence サーバのみポイントできます。

したがって、IM and Presence が LCS/OCS と統合されている場合にハイ アベイラビリティを達成するには、次の図に示すように、IM and Presence サーバと LCS/OCS サーバ間にロード バランサ

を組み込む必要があります。 Cisco CSS11506 Content Services Switch は、IM and Presence が対応している唯一のロード バランサです。

図 *6*：*LCS/OCS* から *IM and Presence* への要求のルーティングのハイ アベイラビリティ



1	ロードバランサは、アクティブ/バックアップモードで動作します。 プライマリ IM and Presence サーバの実行中に、要求がそのサーバにルーティングされ、ハートビート信号を使用して IM and Presence サービスがアライブか確認します。	2	IM and Presence サーバが失敗すると、ロードバランサにより、以降のすべての要求がバックアップ IM and Presence サーバにルーティングされます。

連絡先の検索

パーティション イントラドメイン フェデレーションでは、IM and Presence 対応クライアントと Microsoft Office Communicator の両方で全検索機能を実現しています。

IM and Presence 対応クライアントによる Active Directory（AD）検索は、ユーザがプロビジョニングされた場所に関係なく、ユーザを返します。 Microsoft Office Communicator アドレス帳検索は引

き続き、すべての Microsoft Office Communicator ユーザ、および IM and Presence に移行したあらゆる IM and Presence クライアント ユーザを返します。

連絡先カード情報は、すべての連絡先について両方のクライアントで使用できます。

（注） IM and Presence クライアント ユーザが LCS/OCS でプロビジョニングされていなかった場合、該当ユーザの [msRTCSIP-PrimaryUserAddress] フィールドに対して Active Directory アップデートを実行し、ユーザが Microsoft Office Communicator 検索を使用できるようにします。

ユーザの移行

パーティション イントラドメイン フェデレーション展開の主な利点の 1 つに、企業内で LCS/OCS から IM and Presence へシームレスに遷移できる点があります。 パーティション イントラドメイン フェデレーションには、次のような利点があります。

- IM and Presence クライアント ユーザと Microsoft Office Communicator ユーザが同じプレゼンス情報を共有します。
- ユーザは、その共有ドメイン内でアベイラビリティおよびインスタント メッセージを交換できます。
- ユーザまたは連絡先がプロビジョニングされている場所に関係なく、ユーザは連絡先を検索し、追加できます。

管理者向けの移行プロセスをさらに支援するため、この機能では数多くのツールが使用できます。

ユーザ移行の管理フローは大まかに次のようになります。

1. LCS/OCS ユーザを IM and Presence に移行するライセンスを取得し、割り当てます。
2. LCS/OCS 移行ユーザの LCS/OCS データをバックアップします。
3. 移行する LCS/OCS 各ユーザの LCS/OCS 連絡先リストをエクスポートします。
4. LCS/OCS 移行ユーザの LCS/OCS ユーザ アカウントを無効にします。
5. LCS/OCS 移行ユーザの LCS/OCS ユーザ データを削除します。
6. LCS/OCS 連絡先リストを移行したユーザの IM and Presence データベースにインポートします。
7. 移行したユーザのデスクトップで IM and Presence 対応クライアントを展開します。

ユーザ移行ツール

IM and Presence は、次のユーザ移行手順に対するツールを提供しています。

- 移行する LCS/OCS 各ユーザの LCS/OCS 連絡先リストをエクスポートします。
- LCS/OCS 移行ユーザの LCS/OCS ユーザ アカウントを無効にします。

- LCS/OCS 移行ユーザの LCS/OCS ユーザ データを削除します。
- LCS/OCS 連絡先リストを移行したユーザの IM and Presence データベースにインポートします。

（注） これらのユーザ移行ツールでは、バージョン 1.1 以降の .NET Framework をユーザ移行ツールを実行するサーバにインストールする必要があります。

移行する LCS/OCS 各ユーザの LCS/OCS 連絡先リストをエクスポートする

この IM and Presence ツールを使用して、連絡先リストを LCS/OCS から一括してエクスポートできます。 エクスポートされた連絡先リストは、IM and Presence Contact List Import Bulk Administration Tool（BAT）で承認できるカンマ区切り値（CSV）に書き込まれます。 これらのツールを組み合わせて、連絡先リストを一括管理して、エンドツーエンドで移行できます。

LCS/OCS 移行ユーザの LCS/OCS ユーザ アカウントを無効にする

IM and Presence には、LCS/OCS ユーザ アカウントを一括して無効にするツールが入っています。このツールは、Active Directory に接続し、必要に応じてユーザの LCS/OCS 固有属性を変更することで、LCS/OCS アカウントを無効にします。

LCS/OCS 移行ユーザの LCS/OCS ユーザ データを削除する

LCS/OCS から IM and Presence へパーティション イントラドメイン フェデレーションをルーティングできるようにするため、LCS/OCS ユーザを LCS/OCS から削除する必要があります。 ただし、ユーザが LCS/OCS から削除されると、Microsoft Office Communicator ユーザの連絡先リストからも削除されます。 この IM and Presence ツールは LCS/OCS ユーザ データを一括して削除すると同時に、ユーザが Microsoft Office Communicator ユーザの連絡先リストから削除されないようにします。

LCS/OCS 連絡先リストを移行したユーザの IM and Presence データベースにインポートする

IM and Presence BAT は、連絡先リストの一括インポートに対応するために機能拡張されています。 IM and Presence BAT では、この一括インポートの入力に CSV ファイルが必要です。 LCS/OCS 連絡先リスト エクスポート ツールと共に使用すると、LCS/OCS から IM and Presence へ連絡先リストを移行できます。

（注） ユーザ移行ツールを実行しても、Microsoft Office Communicator にサインインしている他の LCS/OCS ユーザの機能に影響はありません。 ただし、あらかじめスケジュールされたメンテナンスの時間帯にユーザ移行ツールを実行して LCS/OCS および Active Directory システムの負荷を減らすことをお勧めします。

第 2 章

統合の計画

サポート対象のパーティションイントラドメインフェデレーションの統合

この章では、IM and Presence と Microsoft Live Communications Server（LCS）または Microsoft Office Communications Server（OCS）間のパーティション イントラドメイン フェデレーションを有効にする設定手順について説明します。 次に示す LCS および OCS プラットフォームがサポートされています。

- Microsoft Live Communications Server 2005、Standard Edition および Enterprise Edition
- Microsoft Office Communications Server 2007 リリース 2、Standard Edition および Enterprise Edition

関連トピック

ハードウェア要件，（22 ページ）
ソフトウェア要件，（22 ページ）

ハードウェア要件

IM and Presence と LCS/OCS 間のパーティション イントラドメイン フェデレーションでは、次に示すシスコ ハードウェアが必要です。

- IM and Presence サーバ。 IM and Presence ハードウェア サポートについては、IM and Presence 互換性マトリクスを参照してください。
- Cisco Unified Communications Manager サーバ。 Cisco Unified Communications Manager ハードウェア サポートについては、Cisco Unified Communications Manager 互換性マトリクスを参照してください。
- （任意）Cisco CSS11506 Content Services Switch

関連トピック

『Compatibility Information for IM and Presence Service and Cisco Unified Communications Manager』

ソフトウェア要件, （22 ページ）

ソフトウェア要件

次の項では、IM and Presence および LCS/OCS 間のパーティション イントラドメイン フェデレーションに必要なソフトウェアの概要について説明します。

- サーバ ソフトウェア, （22 ページ）
- クライアント ソフトウェア, （23 ページ）

サーバ ソフトウェア

パーティション イントラドメイン フェデレーションには、次に示すサーバ ソフトウェアが必要です。

シスコ ソフトウェア

- IM and Presence Server リリース 9.0
- Cisco Unified Communications Manager Server リリース 9.0

Microsoft ソフトウェア

- 展開に応じて、次のいずれかになります。
  - Microsoft Live Communications Server 2005、Standard または Enterprise Edition
  - Microsoft Office Communications Server 2007 リリース 2、Standard または Enterprise Edition

- 展開に応じて、次のいずれかになります。
  - LCS 管理ツール（LCS のインストール中にオプションのインストール項目が入手可能）
  - OCS 管理ツール（OCS のインストール中にオプションのインストール項目が入手可能）
- Microsoft Active Directory

その他のソフトウェア

バージョン 1.1 以降の .NET Framework：ユーザ移行ツールを実行するサーバにインストールする必要があります。

クライアント ソフトウェア

IM and Presence および LCS/OCS 間のパーティション イントラドメイン フェデレーション展開に必要なクライアント ソフトウェアは、ご使用の展開により異なります。 パーティション イントラドメイン フェデレーション展開では、IM and Presence 対応クライアントを任意に組み合わせることができます。

IM and Presence 対応クライアント

IM and Presence および LCS/OCS 間のパーティション イントラドメイン フェデレーション展開では、次に示す IM and Presence クライアントがサポートされています。

シスコ ソフトウェア

- Cisco Jabber リリース 8.5
- CiscoJabber リリース 8.6
- Cisco Jabber for Mac
- Cisco Jabber for Windows
- Cisco Jabber IM for Mobile（iPhone、Android、Blackberry）
- Cisco Jabber for iPad
- Cisco Jabber for Cius

（注） すべての Cisco Jabber クライアントのバージョンの互換性については、該当する Cisco Jabber クライアントのマニュアルを参照してください。

サードパーティ製ソフトウェア

サードパーティ製の XMPP クライアント

Microsoft LCS/OCS 対応クライアント

展開に応じて、次に示すクライアントがサポートされています。

- Microsoft Office Communicator 2005
- Communicator Web Access 2005

（注） Communicator Web Access 2005 は、IM and Presence および Microsoft LCS 間で TLS 暗号化が有効になっていない場合のみサポートされています。 これは、Communicator Web Access 2005 では、連邦情報処理標準（FIPS）コンプライアンスがサポートされていないためです。FIPS は、必要に応じて IM and Presence による TLSv1 暗号化に対応するため、Microsoft LCS で有効にする必要があります。

- Microsoft Office Communicator 2007 リリース 2
- Communicator Web Access 2007 リリース 2

関連項目

ハードウェア要件, （22 ページ）

統合の準備

IM and Presence および LCS/OCS 間のパーティション イントラドメイン フェデレーションの設定は、慎重に計画することが大切です。 この統合の設定を開始する前に、この項に記載の項目をお読みください。

- プレゼンス ドメイン, （24 ページ）
- ユーザの移行, （25 ページ）
- DNS の設定, （31 ページ）
- 認証局サーバ, （31 ページ）
- ハイ アベイラビリティ, （31 ページ）

プレゼンス ドメイン

パーティション イントラドメイン フェデレーションは、その特性上、共有プレゼンス ドメイン内で IM and Presence および LCS/OCS 間の統合をサポートします。 ただし LCS/OCS は、LCS/OCS 展開ごとに複数のプレゼンス ドメインの設定をサポートします。

（注） すべての Microsoft Office Communicator ユーザのプレゼンス ドメインは、パーティション イントラドメイン フェデレーションの IM and Presence クライアント ユーザと同じでなければなりません。

Microsoft Office Communicator ユーザが同じプレゼンス ドメインを共有していない場合、それらのユーザに対してパーティション イントラドメイン フェデレーションはできません。

ユーザの移行

ユーザが、この統合の一環として LCS/OCS から IM and Presence に移行中の場合、次の点を考慮します。

- 詳細なユーザ移行計画, （25 ページ）
- 移行中のユーザ ID の保守, （28 ページ）
- ユーザ移行ツールの時間に関するガイドライン, （28 ページ）

詳細なユーザ移行計画

IM and Presence および LCS/OCS 間のパーティション イントラドメイン フェデレーション統合は、LCS/OCS から IM and Presence への段階的移行中にユーザ間で基本的な通信を実現するよう設計されています。

ただし、パーティション イントラドメイン フェデレーション統合により、パフォーマンス上のオーバーヘッドが発生します。 このため、IM and Presence は、サーバあたり最大 130,000 件の SIP ドメイン内フェデレーションの連絡先をサポートします。 LCS/OCS から IM and Presence へのユーザ移行中に IM and Presence サーバ上でこのフェデレーションされた連絡先のしきい値を超えないようにするため、詳細な移行計画が必要な場合があります。

次の計算式を使用して、上記のフェデレーションされた連絡先のしきい値を超えずにサポートできる、IM and Presence ユーザの最大数を見積もることができます。

最大対応ユーザ = *130,000*/連絡先リストの平均サイズ

この計算式に基づいて、次の表表 5：IM and Presence の最大対応ユーザ数, （25 ページ） は 130,000 件のフェデレーションされた連絡先のしきい値を超えずにサポートできる、IM and Presence ユーザの最大数を示しています。

表 *5*：*IM and Presence* の最大対応ユーザ数

連絡先リストの平均サイズ	最大対応ユーザ（ハイ アベイラビリティなし）	最大対応ユーザ（ハイ アベイラビリティあり[1]）
200	650	325
150	866	433

連絡先リストの平均サイズ	最大対応ユーザ（ハイ アベイラビリティなし）	最大対応ユーザ（ハイ アベイラビリティあり[1]）
100	1300	650
75	1733	866
50	2600	1300
25	5000	2500

1 これは、アクティブ/アクティブ モードで動作している 2 ノード サブクラスタを想定しています。

ご使用の展開内の IM and Presence サーバでプロビジョニングされるユーザ数が該当の上限値を超える場合、詳細なユーザ移行計画が必要です。 シスコのサポート担当者に連絡し、詳細な移行計画の定義を始めてください。

注意事項

1. 上記の表にある最大対応ユーザ数の値は、最悪の場合の数字、つまりすべての連絡先がフェデレーションされている場合に基づいています。

   適切な移行計画により、130,000 件のフェデレーションされた連絡先のしきい値を超えずに、最大数のユーザを IM and Presence サーバに段階的に展開できます。

2. ハイ アベイラビリティが有効な場合、各 IM and Presence サーバは、IM and Presence 2 ノード サブクラスタ内のすべてのユーザに関連した負荷を処理できなければなりません。 したがって、IM and Presence サーバごとの制限値は半分になるはずです。

3. ご使用の LCS/OCS 展開内の連絡先リスト平均サイズがわからない場合、移行計画が必要かどうか判断している場合に最悪のケース（200 件の連絡先）を想定します。

4. 上記の表にある最大対応ユーザ数の値は、5000 ユーザの IM and Presence OVA テンプレートに基づく HCS-7845-I3 ハードウェアまたは同等のシスコ対応仮想プラットフォームを想定しています。 他のプラットフォームのサブセットに対する同等の数字を次に詳しく説明します。 プラットフォームがリスト上にない場合、シスコのサポート担当者に連絡し、アドバイスを求めてください。

HCS-7825-H4 ハードウェア

IM and Presence は、HCS-7825-H4 プラットフォームで、サーバあたり最大 18,000 件の SIP ドメイン内フェデレーション連絡先をサポートできます。 次の表は、18,000 件のフェデレーションされた連絡先のしきい値を超えずにサポートできる、IM and Presence ユーザの最大数を示しています。

表 *6*：*HCS-7825-H4* ハードウェアの *IM and Presence* 最大対応ユーザ数

連絡先リストの平均サイズ	最大対応ユーザ（ハイ アベイラビリティなし）	最大対応ユーザ（ハイ アベイラビリティあり[2]）
200	90	45
150	120	60
100	180	90
75	240	120
50	360	180
25	720	360
18	1000	500

2 これは、アクティブ/アクティブ モードで動作している 2 ノード サブクラスタを想定しています。

HCS-7845-H2 ハードウェア

IM and Presence は、HCS-7845-H2 プラットフォームで、サーバあたり最大 90,000 件の SIP ドメイン内フェデレーション連絡先をサポートできます。 次の表は、90,000 件のフェデレーションされた連絡先のしきい値を超えずにサポートできる、IM and Presence ユーザの最大数を示しています。

表 *7*：*HCS-7845-H2* ハードウェアの *IM and Presence* 最大対応ユーザ数

連絡先リストの平均サイズ	最大対応ユーザ（ハイ アベイラビリティなし）	最大対応ユーザ（ハイ アベイラビリティあり[3]）
200	450	225
150	600	300
100	900	450
75	1200	600
50	1800	900
25	3600	1800
18	5000	2500

3 これは、アクティブ/アクティブ モードで動作している 2 ノード サブクラスタを想定しています。

関連トピック

ユーザの移行, （18 ページ）

移行中のユーザ ID の保守

LCS/OCS から IM and Presence への移行中、Microsoft Office Communicator ユーザは同じ ID（URI）を保守する必要があります。 移行中に同じ ID を保守する場合、次のような利点があります。

- ユーザの ID が変わらないため、ユーザのアベイラビリティ状態を維持できます。
- 連絡先リストを直接 LCS/OCS から IM and Presence にインポートできるため、ユーザの連絡先リストの移行がさらに簡単になります。

IM and Presence URI は、Cisco Unified Communications Manager のユーザ ID と IM and Presence ドメインを次のように結合して構成されます。

<userid>@<domain>

ユーザが Cisco Unified Communications Manager GUI または Cisco Unified Communications Manager Bulk Administration Tool（BAT）を通して手作業で追加されている場合、ユーザ作成時に指定したユーザ ID がユーザの LCS/OCS URI のユーザ部分と一致していることを確認する必要があります。 たとえば、LCS/OCS URI が bobjones@foo.com の場合、bobjones というユーザ ID を持つユーザを作成する必要があります。

Cisco Unified Communications Manager が Active Directory からのユーザと同期するよう設定されている場合、Cisco Unified Communications Manager のユーザ ID へのマッピングに使用する [Active Directory] フィールドが LCS/OCS URI のユーザ部分と一致していることを確認する必要があります。 次の点に注意してください。

- Cisco Unified Communications Manager は、限定された数の [Active Directory] フィールドの userID とマッピングします。ほとんどの場合、ID は sAMAccountName です。
- Cisco Unified Communications Manager が userID を sAMAccountName にマッピングすると、移行ユーザの LCS/OCS URI も <sAMAccountName>@<domain> というフォーマットに一致します。
- Bob Jones の sAMAccountName が bjones の場合、LCS/OCS URI は bjones@cisco.com でなければなりません。
- 任意の LCS/OCS URI がフォーマット <sAMAccountName>@<domain> に一致しない場合、LCS/OCS から IM and Presence へユーザを初めて移行する前に、それらの URI を変更する必要があります。

ユーザ移行ツールの時間に関するガイドライン

シスコは、LCS/OCS から IM and Presence へユーザを一括して移行できる多数のツールを提供しています。 移行計画を立てるには、多数のユーザを移行している場合に、各ツールが実行するのに必要な時間を知っておくことが重要です。 ここでは、次に示すツールごとの予想実行時間について説明します。

連絡先リスト エクスポート ツール

連絡先リスト エクスポート ツール（ExportContacts.exe）は、平均毎秒 800 件の連絡先（つまり、毎分 48,000 件の連絡先）の速度で LCS/OCS から連絡先をエクスポートできます。 次に示す等式をガイドとして使用し、LCS/OCS ユーザ セットに対するこのツールの予想実行時間を見積もることができます。

連絡先のエクスポート時間（分）= LCS/OCS ユーザ数 x 連絡先リスト平均サイズ/48000

次の表は、多数のサンプル ケースの予想実行時間を示しています。

表 *8*：連絡先リスト エクスポート ツールの予想実行時間サンプル

LCS/OCS ユーザ数	連絡先リストの平均サイズ	連絡先エクスポート時間
2000	100	5 分
5000	75	8 分
15000	60	19 分

アカウント無効化ツール

アカウント無効化ツール（DisableAccount.exe）は、平均毎秒 13 アカウント（毎分 800 アカウント）の速度で LCS/OCS アカウントを無効にできます。 次に示す等式をガイドとして使用し、LCS/OCS ユーザ セットに対するこのツールの予想実行時間を見積もることができます。

アカウントを無効にする時間（分）= LCS/OCS ユーザ数/800

次の表は、多数のサンプル ケースの予想実行時間を示しています。

表 *9*：アカウント無効化ツールの予想実行時間サンプル

LCS/OCS ユーザ数	アカウントを無効にする時間
2000	3 分
5000	7 分
15000	20 分

アカウント削除ツール

アカウント削除ツール（DeleteAccount.exe）は、平均毎秒 13 アカウント（毎分 800 アカウント）の速度で LCS/OCS アカウントを削除できます。 次に示す等式をガイドとして使用し、LCS/OCS ユーザ セットに対するこのツールの予想実行時間を見積もることができます。

アカウントを削除する時間（分）= LCS/OCS ユーザ数/800

次の表は、多数のサンプル ケースの予想実行時間を示しています。

表 *10*：アカウント削除ツールの予想実行時間サンプル

LCS/OCS ユーザ数	アカウントを削除する時間
2000	3 分
5000	7 分
15000	20 分

BAT Contact List Import ツール

IM and Presence BAT ユーティリティは、IM and Presence プラットフォームに応じて、さまざまな速度で連絡先をインポートできます。 次の表は、選択した IM and Presence プラットフォームの予想インポート速度を示しています。

表 *11*：*IM and Presence BAT* ツールのインポート速度

IM and Presence プラットフォーム	インポート速度
MCS-7825-H4/1000 ユーザ OVA	6 秒
MCS-7845-H2	12 秒
MCS-7845-I3/5000 ユーザ OVA	22 秒

次の表は、多数のサンプル ケースの予想実行時間を示しています。

表 *12*：*BAT Contact List Import* ツールの予想実行時間サンプル

ユーザ数	連絡先リストの平均サイズ	インポート時間（速度 = 22 秒）
2000	100	2 時間 32 分
5000	75	4 時間 45 分

ユーザ数	連絡先リストの平均サイズ	インポート時間（速度 = 22 秒）
15000	60	11 時間 22 分

注意事項

1. 連絡先リスト エクスポート ツール、アカウント無効化ツール、およびアカウント削除ツールの計算式は、2Ghz 以上の CPU 処理能力、および 2GB の RAM を備えたハードウェアで実行する LCS/OCS および Active Directory（AD）に基づいています。
2. ユーザ移行ツールを実行しても、Microsoft Office Communicator にサインインしている他の LCS/OCS ユーザの機能に影響はありません。
3. あらかじめスケジュールされたメンテナンスの時間帯にユーザ移行を実行して LCS/OCS および AD システムの負荷を減らすことをお勧めします。

DNS の設定

ドメイン ネーム システム（DNS）の「A」レコードは、すべての IM and Presence および LCS/OCS サーバについて、企業内で公開する必要があります。

LCS/OCS サーバは、すべての IM and Presence サーバの完全修飾ドメイン名（FQDN）および IP アドレスを解決できなければなりません。

同様に、IM and Presence サーバは、すべての LCS/OCS サーバおよびプール FQDN の FQDN および IP アドレスを解決できなければなりません。

（注） IM and Presence では、プレゼンス ドメインが IM and Presence サーバの基礎となるネットワーク ドメインに一致しなければなりません。

認証局サーバ

このパーティション イントラドメイン フェデレーションの一環として TLS 暗号化が有効になっている場合、外部または内部の認証局（CA）を使用して、IM and Presence および LCS/OCS のセキュリティ証明書に署名できます。 同じ CA を使用して LCS/OCS および IM and Presence 証明書に署名することをお勧めします。 そうでない場合、ルート証明書を CA ごとに LCS/OCS および IM and Presence サーバにアップロードする必要があります。

ハイ アベイラビリティ

パーティションイントラドメインフェデレーション展開で、どのようにしてアベイラビリティを設定するか考える必要があります。

IM and Presence パーティション イントラドメイン フェデレーション機能を高度に利用可能にしたい場合、指定の（ルーティング）IM and Presence ノードの前にロード バランサを展開できます。Cisco CSS 11500 Content Services Switch を使用することをお勧めします。

Cisco CSS 11500 Content Services Switch ドキュメントは次の URL から入手できます。

http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_installation_and_configuration_guides_list.html

関連項目

ドメイン内フェデレーションのハイ アベイラビリティ，（13 ページ）

IM and Presence の前提条件の設定

パーティション イントラドメイン フェデレーションの設定を開始する前に、IM and Presence で次のタスクを実行する必要があります。

1. 『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』で説明しているように、IM and Presence をインストールし、設定します。
2. IM and Presence システムが正しく動作しているか、次に示す点を確認します。
   - IM and Presence Troubleshooter を実行します。
   - ローカルな連絡先を IM and Presence に追加できることを確認します。
   - クライアントが IM and Presence サーバからアベイラビリティ状態を受信していることを確認します。

関連トピック

『Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager』

ルーティング IM and Presence サーバに関するその他の設定

マルチサーバ展開では、IM and Presence サーバをルーティング IM and Presence サーバ専用に使用する必要があります。 つまり、このサーバは LCS/OCS からすべての新しい着信 SIP 要求を受け取り、要求の受信者がホームとしている IM and Presence サーバにルーティングするフロントエンド サーバになります。

ユーザは一切ルーティング IM and Presence サーバに割り当てないことをお勧めします。これによりルーティング IM and Presence サーバは、LCS/OCS からの大量の SIP トラフィックを処理する能力を備えることができます。

ルーティング IM and Presence サーバにはユーザは割り当てられないため、多数の機能サービスを非アクティブ化して、ルーティング IM and Presence サーバ上のリソースを解放できます。 ルーティング IM and Presence サーバで次の機能サービスを非アクティブ化します。

- Cisco Presence Engine
- Cisco XCP Text Conference Manager
- Cisco XCP Web Connection Manager
- Cisco XCP Connection Manager
- Cisco XCP SIP Federation Connection Manager
- Cisco XCP XMPP Federation Connection Manager
- Cisco XCP Message Archiver
- Cisco XCP Directory Service
- Cisco XCP Authentication Service

関連項目

ルーティング IM and Presence サーバでの機能サービスの非アクティブ化, （52 ページ）

IM and Presence 機能サービスの開始

パーティションイントラドメインフェデレーションをサポートするには、次のサービスが IM and Presence サーバごとに実行している必要があります。

- Cisco SIP Proxy
- Cisco XCP SIP Federation Connection Manager
- Cisco XCP Router

Cisco XCP Router はネットワーク サービスであるため、デフォルトで開始されます。 Cisco SIP Proxy および Cisco SIP Federation Connection Manager は、開始しなければならない機能サービスです。

次の手順では、Cisco SIP Proxy および Cisco SIP Federation Connection Manager 機能サービスを開始する方法について説明します。 すべての IM and Presence サーバでこの手順を実行する必要があります。

（注） 専用ルーティング IM and Presence サーバについては、Cisco XCP SIP Federation Connection Manager サービスをアクティブにしないでください。専用ルーティング IM and Presence サーバにはユーザは割り当てられていないためです。

手順

ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [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）] メニューで IM and Presence サーバを選択します。

ステップ 3 次のサービスを確認します。

a) Cisco SIP Proxy
b) Cisco SCP SIP Federation Connection Manager

ステップ 4 [保存（Save）] を選択します。

第 3 章

パーティション イントラドメイン フェデレーションの設定ワークフロー

この章では、Microsoft Live Communications Server (LCS) 2005 および Microsoft Office Communications Server (OCS) 2007 R2 を使用したパーティション イントラドメイン フェデレーションの設定ワークフローについて説明します。 LCS/OCS から IM and Presence へのユーザの移行の設定ワークフローについても説明します。

- LCS を使用したパーティション イントラドメイン フェデレーションの設定ワークフロー, 35 ページ
- OCS を使用したパーティション イントラドメイン フェデレーションの設定ワークフロー, 37 ページ
- LCS/OCS から IM and Presence へのユーザ移行の設定ワークフロー, 38 ページ
- IM and Presence と LCS/OCS ドメイン間フェデレーション機能との統合の設定ワークフロー, 39 ページ

LCS を使用したパーティション イントラドメイン フェデレーションの設定ワークフロー

次のワークフローを使用して、IM and Presence および LCS 2005 間のパーティション イントラドメイン フェデレーションを設定します。

IM and Presence の設定

1. パーティション イントラドメイン フェデレーションを有効にする：パーティション イントラドメイン フェデレーション オプションの設定, （41 ページ）を参照してください。
2. LCS 展開へのスタティック ルートの設定：スタティック ルートの設定, （42 ページ）を参照してください。

3 LCS 展開のアクセス コントロール リストの設定：着信アクセス コントロール リストの設定, （44 ページ）を参照してください。

4 （任意）IM and Presence および LCS 間の TLS 暗号化の設定：

a アプリケーション リスナーの設定：アプリケーション リスナーの設定, （46 ページ）を参照してください。

b TLS ピア サブジェクトの設定：TLS ピア サブジェクトの設定, （47 ページ）を参照してください。

c ピア認証 TLS コンテキストの設定：ピア認証 TLS コンテキストの設定, （48 ページ）を参照してください。

d Certificate 認証局（CA）のルート証明書のインポート：認証局のルート証明書のインポート, （49 ページ）を参照してください。

e CA 署名付き証明書の要求：認証局からの署名付き証明書の要求, （50 ページ）を参照してください。

f CA 署名付き証明書のインポート：認証局からの署名付き証明書のインポート, （51 ページ）を参照してください。

5 専用ルーティング IM and Presence サーバを設定している場合、ルーティング IM and Presence サーバの不要な機能サービスを非アクティブ化する：ルーティング IM and Presence サーバでの機能サービスの非アクティブ化, （52 ページ）を参照してください。

LCS の設定

1 ポート 5060 を有効にする：LCS サーバでポート 5060 を有効にする, （69 ページ）を参照してください。

2 IM and Presence 展開へのスタティック ルートの設定：LCS スタティック ルートが IM and Presence をポイントするように設定, （70 ページ）を参照してください。

3 IM and Presence 展開のホスト認証の追加：LCS で IM and Presence 用のホスト認証を追加, （71 ページ）を参照してください。

4 （任意）IM and Presence および LCS 間の TLS 暗号化の設定：

a 連邦情報処理標準コンプライアンスを LCS サーバごとに有効にする：連邦情報処理標準コンプライアンスを LCS で有効にする, （74 ページ）を参照してください。

b TLS 相互認証を LCS サーバごとに設定されるようにする：LCS 上での相互 TLS 認証の設定, （75 ページ）を参照してください。

c CA ルート証明書が LCS サーバごとにインストールされるようにする：LCS への認証局のルート証明書のインストール, （76 ページ）を参照してください。

d すべての LCS サーバに必要な署名付き証明書を持たせる：既存の LCS 署名付き証明書の検証, （78 ページ）を参照してください。

e 必要な場合、新しい署名付き証明書を要求する：認証局からの署名付き証明書の要求, （79 ページ）を参照してください。

5 サービスの再起動：LCS サーバでのサービスの再起動, （73 ページ）を参照してください。

OCS を使用したパーティション イントラドメイン フェデレーションの設定ワークフロー

次のワークフローを使用して、IM and Presence および OCS（2007 および 2007 R2）間のパーティション イントラドメイン フェデレーションを設定します。

IM and Presence の設定

1. パーティション イントラドメイン フェデレーションを有効にする：パーティション イントラドメイン フェデレーション オプションの設定, （41 ページ）を参照してください。
2. OCS 展開へのスタティック ルートの設定：スタティック ルートの設定, （42 ページ）を参照してください。
3. OCS 展開のアクセス コントロール リストの設定：着信アクセス コントロール リストの設定, （44 ページ）を参照してください。
4. （任意）IM and Presence および OCS 間の TLS 暗号化の設定：
   a. アプリケーション リスナーの設定：アプリケーション リスナーの設定, （46 ページ）を参照してください。
   b. TLS ピア サブジェクトの設定：TLS ピア サブジェクトの設定, （47 ページ）を参照してください。
   c. ピア認証 TLS コンテキストの設定：ピア認証 TLS コンテキストの設定, （48 ページ）を参照してください。
   d. Certificate 認証局（CA）のルート証明書のインポート：認証局のルート証明書のインポート, （49 ページ）を参照してください。
   e. CA 署名付き証明書の要求：認証局からの署名付き証明書の要求, （50 ページ）を参照してください。
   f. CA 署名付き証明書のインポート：認証局からの署名付き証明書のインポート, （51 ページ）を参照してください。
5. 専用ルーティング IM and Presence サーバを設定している場合、ルーティング IM and Presence サーバの不要な機能サービスを非アクティブ化します。 ルーティング IM and Presence サーバでの機能サービスの非アクティブ化, （52 ページ）を参照してください。

OCS の設定

1. ポート 5060 を有効にする：OCS サーバでポート 5060 を有効にする, （55 ページ）を参照してください。
2. IM and Presence 展開へのスタティック ルートの設定：IM and Presence をポイントするよう OCS スタティック ルートを設定する, （56 ページ）を参照してください。
3. IM and Presence 展開のホスト認証の追加：IM and Presence の OCS でのホスト認証の追加, （57 ページ）を参照してください。

4 （任意）IM and Presence および OCS 間の TLS 暗号化の設定：

a 連邦情報処理標準コンプライアンスを OCS サーバごとに有効にする：連邦情報処理標準コンプライアンスを OCS で有効にする，（60 ページ）を参照してください。

b TLS 相互認証を OCS サーバごとに設定されるようにする：TLS 相互認証の OCS での設定，（60 ページ）を参照してください。

c CA ルート証明書が OCS サーバごとにインストールされるようにする：認証局ルート証明書の OCS へのインストール，（61 ページ）を参照してください。

d すべての OCS サーバに必要な署名付き証明書を持たせる：既存の OCS 署名付き証明書の検証，（64 ページ）を参照してください。

e 必要な場合、新しい署名付き証明書を要求する：認証局からの署名付き証明書の要求，（65 ページ）を参照してください。

5 サービスの再起動：OCS フロントエンド サーバでのサービスの再起動，（58 ページ）を参照してください。

LCS/OCS から IM and Presence へのユーザ移行の設定ワークフロー

次のワークフローを使用して、LCS/OCS から IM and Presence へユーザを移行します。

1 ユーザ移行ツールのダウンロード：シスコのユーザ移行ツール，（83 ページ）を参照してください。

2 無制限の連絡先リスト サイズおよびウォッチャ サイズを IM and Presence で設定する：無制限の連絡先リストとウォッチャの設定，（84 ページ）を参照してください。

3 登録要求の自動認証を有効にする：サブスクリプション要求の自動許可の有効化，（85 ページ）を参照してください。

4 移行ユーザの IM and Presence でのプロビジョニング：Cisco Unified Communications Manager 上での LCS/OCS ユーザのプロビジョニング，（86 ページ）を参照してください。

5 移行ユーザの LCS/OCS データのバックアップ：ユーザ LCS/OCS の連絡先リスト情報のバックアップ，（86 ページ）を参照してください。

6 移行ユーザの LCS/OCS 連絡先リストのエクスポート：ユーザを移行するための連絡先リストのエクスポート，（87 ページ）を参照してください。

7 移行ユーザの LCS/OCS アカウントを無効にする：LCS/OCS でのユーザの無効化，（92 ページ）を参照してください。

8 移行ユーザの LCS/OCS アカウントが無効になっていることを確認する：Active Directory の更新が LCS/OCS と同期していることの確認，（94 ページ）を参照してください。

9 移行ユーザの LCS/OCS ユーザ データの削除：ユーザを移行するためのデータベースからのユーザ データの削除，（95 ページ）を参照してください。

10 移行ユーザの連絡先リストを IM and Presence にインポートする：IM and Presence にユーザを移行するための連絡先リストのインポート，（97 ページ）を参照してください。

11 連絡先リストおよび IM and Presence のウォッチャ制限をリセットする：連絡先リストと最大ウォッチャの最大サイズのリセット，（99 ページ）を参照してください。

IM and Presence と LCS/OCS ドメイン間フェデレーション機能との統合の設定ワークフロー

（注） このワークフローを開始する前に、LCS/OCS とのパーティション イントラドメイン フェデレーションを設定し、正しく動作するようにします。 ご使用の展開内でのパーティション イントラドメイン フェデレーションの設定については、該当するワークフローを参照してください。

1 IM and Presence のフェデレーション ドメインをそれぞれ設定する：リモート ドメインの SIP フェデレーション ドメインとしての設定，（101 ページ）を参照してください。

2 スタティック ルートを IM and Presence の各リモート ドメインに設定する：リモート ドメインのスタティック ルートの設定，（102 ページ）を参照してください。

第 4 章

IM and Presence Server for Partitioned Intradomain Federation の設定

パーティション イントラドメイン フェデレーション オプションの設定

次の手順では、IM and Presence でパーティション イントラドメイン フェデレーションを有効にし、ルーティング モードを設定する方法について説明します。

（注） マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。パーティション イントラドメイン フェデレーションを有効にする、またはルーティング モードを選択する場合、これらの設定はクラスタ全体で有効になります。したがって、ある指定のクラスタ内の IM and Presence パブリッシャ ノードでのみ有効にする必要があります。

手順

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

ステップ 2 [LCS/OCS とのパーティション イントラドメイン フェデレーションを有効にする（Enable Partitioned Intradomain Federation with LCS/OCS）] をオンにします。

ステップ 3 警告メッセージを読んで、[OK] を選択します。

ステップ 4 [パーティション イントラドメイン フェデレーション ルーティング モード（Partitioned Intradomain Federation Routing Mode）] ドロップダウン リストから次のいずれかを選択します。

- 基本ルーティングモード（Basic Routing Mode）（デフォルト）
- 高度ルーティングモード（Advanced Routing Mode）

ステップ 5 [保存（Save）] を選択します。

ステップ 6 パーティション イントラドメイン フェデレーションを有効にした、またはルーティング モードを選択した後、クラスタのすべての IM and Presence ノードの Cisco CP Router を再起動する必要があります。 Cisco XCP ルータを再起動するには、[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）] を選択します。

関連トピック

IM and Presence から LCS/OCS への要求のルーティング, （7 ページ）

スタティック ルートの設定

次の手順では、スタティック ルートを設定し、IM and Presence および Microsoft Live Communications Server（LCS）または Microsoft Office Communications Server（OCS）間のパーティション イントラドメイン フェデレーション ルーティングを有効にする方法について説明します。 次に示す LCS/OCS エンティティごとにスタティック ルートを個々に追加する必要があります。

- OCS/IM and Presence ドメイン
- 各 LCS/OCS Enterprise Edition フロントエンド サーバまたは Standard Edition サーバ FQDN
- 各 LCS/OCS プール FQDN（Enterprise Edition のみ）

OCS/IM and Presence ドメインのスタティック ルートについては、次の点に注意してください。

- Standard Edition LCS/OCS の場合、スタティック ルートは特定の Standard Edition サーバの IP アドレスをポイントする必要があります。
- Enterprise Edition LCS/OCS の場合、スタティック ルートは、特定の LCS/OCS Enterprise Edition フロントエンド サーバまたはフロントエンド ロード バランサの IP アドレスをポイントする

必要があります（LCS/OCS フロントエンド ロード バランサからルーティングしている場合）。

Enterprise Edition LCS/OCS プール FQDN スタティック ルートの場合、スタティック ルートは、そのプール内の特定のフロントエンド サーバ、またはそのプールのフロントエンド ロード バランサの IP アドレスをポイントする必要があります（LCS/OCS フロントエンド ロード バランサからルーティングしている場合）。

IM and Presence は、LCS/OCS フロントエンド ロード バランサとして Cisco Application Control Engine（ACE）を使用してテストされています。ACE の代わりに他のロードバランサを使用できます。認定されたロード バランサのリストについては次の URL を参照してください。http://technet.microsoft.com/en-us/office/ocs/cc843611 ただし、それらのロード バランサを導入し、正しく管理するのはお客様の責任です。

（注） シスコでは、ACE 以外のロード バランサをポイントするスタティック ルートの設定はサポートしていません。

ACE が設定されたフロントエンドのロードバランサでないような導入環境では、フロントエンド ロードバランサをバイパスするためのスタティック ルートを設定することをお勧めします。

ハイ アベイラビリティを目指し、次のバックアップ スタティック ルートを追加で設定できます。

- OCS/IM and Presence ドメイン
- 各 LCS/OCS プール FQDN（LCS/OCS フロントエンド ロード バランサをバイパスする場合は Enterprise Edition のみ）

バックアップ ルートの優先順位は低く、プライマリ スタティック ルートの次のホップ アドレスに到達できない場合にのみ使用されます。

（注） マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。これらの設定はクラスタ全体で有効になります。したがって、ある指定のクラスタ内の IM and Presence パブリッシャ ノードでのみ設定する必要があります。

手順

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

ステップ 3 ドメイン、つまり FQDN が元に戻るよう [宛先パターン（Destination Pattern）] 値を入力します。次に例を示します。

- ドメインが domaina.com の場合、[宛先パターン（Destination Pattern）] 値は .com.domaina でなければなりません。
- FQDN が name1.name2.domain.com の場合、[宛先パターン（Destination Pattern）] 値は .com.domain.name2.name1 でなければなりません。

ステップ 4 [ルート タイプ（Route Type）] で [ドメイン（domain）] を選択します。

ステップ 5 [ネクスト ホップ（Next Hop）] フィールドに LCS/OCS サーバの IP アドレスを入力します。

ステップ 6 [ネクスト ホップ ポート（Next Hop Port）] および [プロトコル タイプ（Protocol Type）] を次のように設定します。

- TLS 暗号化の場合：
- [ネクスト ホップ ポート（Next Hop Port）] の番号は **5061**
- [プロトコル タイプ（Protocol Type）] は、**TLS**
- TCP の場合：
- [ネクスト ホップ ポート（Next Hop Port）] の番号は **5060**
- [プロトコル タイプ（Protocol Type）] は、**TCP**

ステップ 7 [プライオリティ（Priority）] 値を次のように入力します。

- プライマリ スタティック ルートについては、デフォルトの [プライオリティ（Priority）] 値 **1** を入力します。
- バックアップ スタティック ルートについては、1 より大きい [プライオリティ（Priority）] 値を入力します （値が小さいほど、スタティック ルートのプライオリティは上がります）。

ステップ 8 他のすべてのパラメータにはデフォルト値を選択します。

ステップ 9 [保存（Save）] を選択します。

着信アクセス コントロール リストの設定

次の手順では、LCS/OCS サーバが認証されなくても IM and Presence サーバにアクセスできるよう、着信アクセスコントロールリスト（ACL）のエントリを設定する方法について説明します。

着信 ACL の設定方法は、どの程度厳格に IM and Presence へのアクセスを制御するかにより異なります。

- IM and Presence へオープン アクセスできるようにする場合は、アドレス パターンが [すべて（All）] のエントリを追加できます。

- 特定のネットワーク ドメインから IM and Presence へアクセスできるようにする場合は、アドレス パターンが特定のドメインに一致するエントリを追加できます。 たとえば、foo.com 内の任意のサーバからアクセスできるようにするには、アドレス パターンに **foo.com** を入力します。
- 特定のサーバから IM and Presence へアクセスできるようにする場合は、アドレス パターンが特定の IP アドレス、またはそれらのサーバの FQDN に一致するエントリを追加できます。 たとえば、特定のサーバ ocs1.foo.com からアクセスできるようにするには、アドレス パターンに **ocs1.foo.com** を入力します。

パーティション イントラドメイン フェデレーションについては、IM and Presence へのアクセスを OCS FQDN または IP アドレスのみに制限することにした場合、次に示すエンティティの ACL エントリを追加する必要があります。

- 各 LCS/OCS Enterprise Edition フロントエンド サーバまたは Standard Edition サーバ
- 各 LCS/OCS プール FQDN（Enterprise Edition のみ）

（注） マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。これらの設定はクラスタ全体で有効になります。したがって、ある指定のクラスタ内の IM and Presence パブリッシャ ノードでのみ設定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）] > [着信 ACL（Incoming ACL）] を選択します。

ステップ 2 [新規追加（Add New）] を選択します。

ステップ 3 [説明（Description）] フィールドに、OCS Server など、エントリの説明を入力します。

ステップ 4 [アドレス パターン（Address Pattern）] フィールドに、次のいずれかを入力します。

- すべて（All）
- <domain_name>
- <IP_Address>
- <FQDN>

ステップ 5 [保存（Save）] を選択します。

TLS 暗号化の設定

IM and Presence および LCS/OCS 間の TLS 暗号化を設定するには、次の手順を実行する必要があります。

（注） マルチクラスタ展開をしている場合、クラスタごとにこの手順を実行する必要があります。これらの設定はクラスタ全体で有効になります。したがって、ある指定のクラスタ内の IM and Presence パブリッシャ ノードでのみ設定する必要があります。

アプリケーション リスナーの設定

IM and Presence は、デフォルトでポート 5062 でピア（相互）TLS 認証を行います。 ポート 5061 でピア TLS 認証が行われるようにするには、このデフォルト設定を変更する必要があります。 次の手順は、この変更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）] > [システム（System）] > [アプリケーション リスナー（Application Listeners）] を選択します。

ステップ 2 アプリケーション リスナーがまだ表示されていない場合、[検索（Find）] を選択して、すべてのアプリケーション リスナーを表示します。

ステップ 3 [デフォルト Cisco SIP Proxy TLS リスナー - サーバ認証（Default Cisco SIP Proxy TLS Listener – Server Auth）] を選択します。

ステップ 4 [ポート（Port）] 値を **5063** に変更します。

ステップ 5 [保存（Save）] を選択し、表示されるポップアップ ウィンドウで [OK] を選択します。

ステップ 6 [関連リンク（Related Links）] ドロップダウン リストで、[検索/一覧表示に戻る（Back to Find/List）] を選択し、[OK] を選択してアプリケーション リスナー リストに戻ります。

ステップ 7 [デフォルト Cisco SIP Proxy TLS リスナー - ピア認証（Default Cisco SIP Proxy TLS Listener – Peer Auth）] を選択します。

ステップ 8 [ポート（Port）] 値を **5061** に変更します。

ステップ 9 [保存（Save）] を選択し、表示されるポップアップ ウィンドウで [OK] を選択します。

ステップ 10 [関連リンク（Related Links）] ドロップダウン リストで、[検索/一覧表示に戻る（Back to Find/List）] を選択し、[OK] を選択してアプリケーション リスナー リストに戻ります。

ステップ 11 [デフォルト Cisco SIP Proxy TLS リスナー - サーバ認証（Default Cisco SIP Proxy TLS Listener – Server Auth）] を選択します。

ステップ 12 [ポート（Port）] 値を **5062** に変更します。

ステップ 13 [保存（Save）] を選択します。

ステップ 14 クラスタのすべての IM and Presence ノードで SIP Proxy サービスを再起動します。 SIP Proxy サービスを再起動するには、[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）] を選択します。

次の作業

TLS ピア サブジェクトの設定, （47 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

TLS ピア サブジェクトの設定

ピア TLS 認証の場合、IM and Presence では、ピアにより提示されるセキュリティ証明書から件名共通名（CN）が [TLS ピア サブジェクト（TLS Peer Subject）] リストに含まれている必要があります。 次の手順では、このリストに件名 CN を追加する手順について説明します。

パーティション イントラドメイン フェデレーションについては、次に示すエンティティの TLS ピア サブジェクトを追加する必要があります。

- 各 LCS/OCS Enterprise Edition フロントエンド サーバまたは Standard Edition サーバ
- 各 LCS/OCS プール完全修飾ドメイン名（FQDN）（Enterprise Edition のみ）

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）] を選択します。

ステップ 3 ピア サブジェクト名については、IM and Presence に表示される証明書の件名 CN を入力します。

ステップ 4 [説明（Description）] フィールドに、OCS Server など、件名の説明を入力します。

ステップ 5 [保存（Save）] を選択します。

ステップ 6 クラスタのすべての IM and Presence ノードで SIP Proxy サービスを再起動します。 SIP Proxy サービスを再起動するには、[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）] を選択します。

次の作業

ピア認証 TLS コンテキストの設定, （48 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

ピア認証 TLS コンテキストの設定

IM and Presence および LCS/OCS 間の TLS 暗号化をサポートするには、IM and Presence のピア認証 TLS コンテキスト設定を変更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 コンテキスト設定（TLS Context Configuration）] を選択します。

ステップ 2 [検索（Find）] を選択します。

ステップ 3 [デフォルト Cisco SIP Proxy ピア認証 TLS コンテキスト（Default Cisco SIP Proxy Peer Auth TLS Context）] を選択します。

ステップ 4 [空の TLS フラグメントの無効化（Disable Empty TLS Fragments）] チェックボックスがオフになっていることを確認します。

ステップ 5 使用可能な TLS 暗号のリストから、すべての暗号を選択します。

ステップ 6 [右へ移動（Move Right）] 矢印を選択して、選択されたこれらの暗号を [選択された TLS 暗号（Selected TLS Ciphers）] リストに移動します。

ステップ 7 使用可能な TLS ピア サブジェクトのリストから、TLS ピア サブジェクトの設定, （47 ページ）で設定した TLS ピア サブジェクトを選択します。

ステップ 8 [右へ移動（Move Right）] 矢印を選択して、選択された TLS ピア サブジェクトを [選択された TLS ピア サブジェクト（Selected TLS Peer Subjects）] リストに移動します。

ステップ 9 [保存（Save）] を選択します。

ステップ 10 クラスタのすべての IM and Presence ノードで SIP Proxy サービスを再起動します。 SIP Proxy サービスを再起動するには、[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）] を選択します。

次の作業

認証局のルート証明書のインポート, （49 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

認証局のルート証明書のインポート

通常、すべての LCS/OCS セキュリティ証明書は認証局（CA）により署名されています。 IM and Presence 証明書も、LCS/OCS で使用されている同じ認証局で署名する必要があります。 IM and Presence が LCS/OCS CA で署名された証明書を使用、その同じ CA で署名された LCS/OCS 証明書を承認するには、CA のルート証明書を IM and Presence 信頼ストアにアップロードする必要があります。

はじめる前に

ルート証明書をインポートする前に、認証局から証明書を取得し、それをローカル コンピュータにコピーします。

手順

ステップ 1 IM and Presence で [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）] > [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）] を選択します。

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

ステップ 4 [ルート証明書（Root Certificate）] フィールドは空白のままにします。

ステップ 5 [説明（Description）] フィールドに、「認証局のルート証明書」など、証明書の説明を入力します。

ステップ 6 [参照（Browse）] を選択して、ローカル コンピュータ上のルート証明書を見つけます。

ステップ 7 [ファイルのアップロード（Upload File）] を選択し、証明書を IM and Presence サーバにアップロードします。

ステップ 8 クラスタのすべての IM and Presence ノードで SIP Proxy サービスを再起動します。 SIP Proxy サービスを再起動するには、[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）] を選択します。

次の作業

認証局からの署名付き証明書の要求, （50 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

認証局からの署名付き証明書の要求

IM and Presence 証明書は、LCS/OCS で使用されている同じ認証局で署名する必要があります。CA 署名付き証明書を入手するには、次に示す 2 段階のプロセスを実行する必要があります。

手順

ステップ 1 IM and Presence 証明書署名要求（CSR）を生成します。

ステップ 2 CA 署名付き証明書を IM and Presence にアップロードします。
次の手順では、IM and Presence から CSR を生成して、ダウンロードする方法について説明します。 IM and Presence CSR は 2048 ビットです。

ステップ 3 IM and Presence で [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）] > [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 4 [CSR の作成（Generate CSR）] を選択します。

ステップ 5 [証明書の名前（Certificate Name）] ドロップダウン リストで、**cup** を選択します。

ステップ 6 [CSR の作成（Generate CSR）] を選択します。

ステップ 7 [ステータス（Status）] に「成功：証明書署名要求が作成されました（Success: Certificate Signing Request Generated）」と表示されている場合、[閉じる（Close）] を選択します。

ステップ 8 [CSR のダウンロード（Download CSR）] を選択します。

ステップ 9 [証明書の名前（Certificate Name）] ドロップダウン リストで、**cup** を選択します。

ステップ 10 [CSR のダウンロード（Download CSR）] を選択し、証明書をローカル コンピュータにダウンロードします。

ステップ 11 証明書がダウンロードされたら、[閉じる（Close）] を選択します。

（注） CSR をダウンロードしたら、それを使用して選択した CA から署名付き証明書を要求できます。 これは、有名なパブリック CA または内部 CA の場合があります。

次の作業

認証局からの署名付き証明書のインポート, （51 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

認証局からの署名付き証明書のインポート

次の手順では、CA 署名付き証明書を IM and Presence にアップロードする方法について説明します。

はじめる前に

IM and Presence から CSR を生成し、ダウンロードします。 認証局からの署名付き証明書の要求, （50 ページ）を参照してください。

手順

ステップ 1 IM and Presence で [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）] > [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）] を選択します。

ステップ 3 [証明書の名前（Certificate Name）] ドロップダウン リストで、**cup** を選択します。

ステップ 4 [ルート証明書（Root Certificate）] フィールドに、認証局からの署名付き証明書の要求, （50 ページ）でダウンロードしたルート証明書のファイル名を入力します。

ステップ 5 [説明（Description）] フィールドに、「CA 署名付き証明書」など、証明書の説明を入力します。

ステップ 6 [参照（Browse）] を選択して、ローカル コンピュータ上の証明書ファイルを見つけます。

ステップ 7 [ファイルのアップロード（Upload File）] を選択し、証明書を IM and Presence サーバにアップロードします。

ステップ 8 証明書をアップロードしたら、クラスタのすべての IM and Presence ノードで SIP Proxy サービスを再起動します。 SIP Proxy サービスを再起動するには、[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）] を選択します。

関連トピック

統合のトラブルシューティング, （107 ページ）

ルーティング IM and Presence サーバでの機能サービスの非アクティブ化

ルーティング IM and Presence サーバが LCS/OCS からの SIP トラフィックを処理できる容量を備えるには、ユーザをルーティング IM and Presence サーバに割り当ててはいけません。 つまり、割り当てユーザをサポートしている多数の IM and Presence 機能サービスをルーティング IM and Presence サーバで非アクティブ化できるということです。 これらのサービスを非アクティブ化すると、ルーティング IM and Presence サーバは、その SIP ルーティングの役割を果たすために処理能力が追加されます。 次の手順では、機能サービスを非アクティブ化する方法について説明します。

手順

ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [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）] メニューでルーティング IM and Presence サーバを選択します。

ステップ 3 次の機能サービスのチェックボックスをそれぞれオフにします。

- Cisco Presence Engine
- Cisco XCP Text Conference Manager
- Cisco XCP Web Connection Manager
- Cisco XCP Connection Manager
- Cisco XCP SIP Federation Connection Manager
- Cisco XCP XMPP Federation Connection Manager
- Cisco XCP Message Archiver
- Cisco XCP Directory Service
- Cisco XCP Authentication Service

ステップ 4 [保存（Save）] を選択します。

関連トピック

ルーティング IM and Presence サーバに関するその他の設定, （32 ページ）

第 5 章

Microsoft Office Communications Server for Partitioned Intradomain Federation の設定

（注） この章の手順は、Microsoft Office Communications Server (OCS) 2007 R2 にのみ適用されます。

OCS サーバでポート 5060 を有効にする

IM and Presence および OCS 間の SIP トラフィックについて暗号化されていない TCP 接続を使用する場合、TCP SIP ポート 5060 をリッスンするよう OCS を設定する必要があります。 次の手順では、OCS サーバでポート 5060 を有効にする方法について説明します。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンド サーバでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 Standard Edition または Enterprise Edition フロントエンド サーバの FQDN を右クリックし、[プロパティ（Properties）] > [フロントエンドのプロパティ（Front End Properties）] を選択します。

ステップ 3 [全般（General）] タブをクリックします。

ステップ 4 [接続（Connections）] にポート 5060 が記載されていない場合は、[追加（Add）] を選択します。

ステップ 5 [IP アドレス（IP Address）] 値に **All** を選択します。

ステップ 6 [ポート（Port）] 値に **5060** を選択します。

ステップ 7 [トランスポート（Transport）] 値に **TCP** を選択します。

ステップ 8 [OK] をクリックして、[接続の追加（Add Connection）] ウィンドウを閉じます。 これで、ポート 5060 が [接続（Connections）] リストに記載されているはずです。

ステップ 9 [OK] を再度選択して、[フロントエンド サーバ プロパティ（Front End Server Properties）] ウィンドウを閉じます。

次の作業

IM and Presence をポイントするよう OCS スタティック ルートを設定する，（56 ページ）

関連トピック

統合のトラブルシューティング，（107 ページ）

IM and Presence をポイントするよう OCS スタティック ルートを設定する

OCS が要求を IM and Presence にルーティングできるようにするには、OCS サーバでスタティック ルートを設定する必要があります。 スタティック ルートは IM and Presence をポイントします。 次の手順は、必要なスタティック ルートを設定する方法を説明します。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのプールでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 適宜 Enterprise Edition プール名または Standard Edition サーバ名を右クリックします。

ステップ 3 [プロパティ（Properties）]>[フロントエンドのプロパティ（Front End Properties）] を選択します。

ステップ 4 [ルーティング（Routing）] タブを選択し、[追加（Add）] を選択します。

ステップ 5 foo.com など、IM and Presence サーバのドメインを入力します。

ステップ 6 [電話の URI（Phone URI）] チェックボックスがオフになっていることを確認します。

ステップ 7 IM and Presence サーバの IP アドレスをネクスト ホップの IP アドレスとして入力します。

ステップ 8 [ネクスト ホップ トランスポート（Next Hop Transport）] 値に **TCP** を選択します。

ステップ 9 [ネクスト ホップ ポート（Next Hop Port）] 値に **5060** を入力します。

ステップ 10 [要求 URI 内のホストを置き換える（Replace host in request URI）] チェックボックスがオフになっていることを確認します。

ステップ 11 [OK] をクリックして、[静的ルートの追加（Add Static Route）] ウィンドウを閉じます。 新しいスタティック ルートがルーティング リストに表示されるはずです。

ステップ 12 [OK] を再度選択して、[フロントエンド サーバ プロパティ（Front End Server Properties）] ウィンドウを閉じます。

次の作業

IM and Presence の OCS でのホスト認証の追加, （57 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

IM and Presence の OCS でのホスト認証の追加

認証を求められずに OCS が IM and Presence から SIP 要求を承認できるようにするには、IM and Presence サーバごとに OCS でホスト認証エントリを設定する必要があります。

OCS および IM and Presence 間の TLS 暗号化を設定している場合、次のように IM and Presence サーバごとに 2 つのホスト認証エントリを追加する必要があります。

- 最初のエントリには、IM and Presence サーバの FQDN が含まれている必要があります。
- 2 つ目のエントリには、IM and Presence サーバの IP アドレスが含まれている必要があります。

TLS 暗号化を設定していない場合、IM and Presence サーバごとにホスト認証エントリを 1 つだけ追加します。 このホスト認証エントリには、IM and Presence サーバの IP アドレスが含まれている必要があります。

次の手順では、必要なホスト認証エントリを追加する方法について説明します。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのプールでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 適宜 Enterprise Edition プール名または Standard Edition サーバ名を右クリックします。

ステップ 3 [プロパティ（Properties）] > [フロントエンドのプロパティ（Front End Properties）] を選択します。

ステップ 4 [ホストの承認（Host Authorization）] タブを選択して、[追加（Add）] を選択します。

ステップ 5 FQDN を入力している場合、[FQDN] を選択して、IM and Presence サーバの FQDN を入力します。たとえば、cup1.foo.com などです。

ステップ 6 IP アドレスを入力する場合は、[IP アドレス（IP Address）] を選択し、IM and Presence サーバの IP アドレスを入力します。 たとえば、10.x.x.x などです。

ステップ 7 [送信のみ（Outbound Only）] チェックボックスがオフになっていることを確認します。

ステップ 8 [サーバとして帯域を制限する（Throttle as Server）] チェックボックスをオンにします。

ステップ 9 [認証済みとして扱う（Treat as Authenticated）] をオンにします。

ステップ 10 [OK] をクリックして、[承認済みホストの追加（Add Authorized Host）] ウィンドウを閉じます。

ステップ 11 IM and Presence サーバごとに手順 4 ～ 10 を繰り返します。

ステップ 12 すべてのホスト認証エントリを追加したら、[OK] を選択して、[フロントエンドサーバプロパティ（Front End Server Properties）] ウィンドウを閉じます。

次の作業

OCS フロントエンド サーバでのサービスの再起動, （58 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

OCS フロントエンド サーバでのサービスの再起動

OCS ですべての設定手順が完了したら、OCS サービスを再起動し、設定を有効にする必要があります。

（注）
- この手順は、あらかじめスケジュールされたメンテナンスの時間帯に実施することをお勧めします。
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンド サーバでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 Standard Edition サーバまたは Enterprise Edition フロントエンド サーバの FQDN を右クリックし、[停止（Stop）] > [フロントエンド サービス（Front End Services）] > [フロントエンド サービス（Front End Service）] を選択します。

ステップ 3 サービスが停止したら、Standard Edition サーバまたは Enterprise Edition フロントエンド サーバの FQDN を右クリックし、[開始（Start）] > [フロントエンド サービス（Front End Services）] > [フロントエンド サービス（Front End Service）] を選択します。

関連トピック

統合のトラブルシューティング, （107 ページ）

TLS 暗号化の設定

IM and Presence および OCS 間の TLS 暗号化を設定するには、次の手順を実行する必要があります。

- 連邦情報処理標準コンプライアンスを OCS で有効にする, （60 ページ）
- TLS 相互認証の OCS での設定, （60 ページ）
- 認証局ルート証明書の OCS へのインストール, （61 ページ）
- 既存の OCS 署名付き証明書の検証, （64 ページ）
- 認証局からの署名付き証明書の要求, （65 ページ）

TLS の設定が完了したら、OCS サーバでサービスを再起動する必要があります。OCS フロントエンド サーバでのサービスの再起動, （58 ページ）を参照してください。

連邦情報処理標準コンプライアンスを OCS で有効にする

IM and Presence および OCS 間の TLS 暗号化をサポートするには、OCS サーバで TLSv1 を有効にする必要があります。 TLSv1 は連邦情報処理標準（FIPS）コンプライアンスの一環として Windows サーバに組み込まれています。 次の手順では、FIPS コンプライアンスを有効にする方法について説明しています。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンド サーバでこの手順を実行する必要があります。

手順

ステップ 1 OCS サーバで、[スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [ローカル セキュリティ ポリシー（Local Security Policy）] を選択します。

ステップ 2 コンソール ツリーから、[ローカル ポリシー（Local Policies）] を選択します。

ステップ 3 [セキュリティ オプション（Security Options）] を選択します。

ステップ 4 [システム暗号化：暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う（System Cryptography: Use FIPS Compliant algorithms for encryption, hashing and signing）] をダブルクリックします。

ステップ 5 セキュリティ設定を有効にします。

ステップ 6 [OK] を選択します。

ステップ 7 [ローカル セキュリティの設定（Local Security Setting）] ウィンドウを閉じます。

次の作業

TLS 相互認証の OCS での設定, （60 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

TLS 相互認証の OCS での設定

IM and Presence および OCS 間の TLS 暗号化を設定するには、TLS 相互認証について OCS サーバでポート 5061 を設定する必要があります。 次の手順では、相互 TLS 認証用にポート 5061 を設定する方法について説明します。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンドサーバでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 Standard Edition サーバまたは Enterprise Edition フロントエンド サーバの FQDN を右クリックし、[プロパティ（Properties）] > [フロントエンドのプロパティ（Front End Properties）] を選択します。

ステップ 3 [全般（General）] タブを選択します。

ステップ 4 ポート 5061 に関連付けられた転送が **MTLS** の場合、手順 8 に進みます。

ステップ 5 ポート 5061 に関連付けられた転送が **MTLS** ではない場合、[編集（Edit）] を選択します。

ステップ 6 [転送（Transport）] ドロップダウン リストから **MTLS** を選択します。

ステップ 7 [OK] をクリックして、[接続の編集（Edit Connection）] ウィンドウを閉じます。 これで、ポート 5061 に関連付けられた転送は **MTLS** になるはずです。

ステップ 8 [OK] を選択して [プロパティ（Properties）] ウィンドウを閉じます。

次の作業

認証局ルート証明書の OCS へのインストール, （61 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

認証局ルート証明書の OCS へのインストール

IM and Presence および OCS 間の TLS 暗号化をサポートするには、OCS サーバごとに署名付きセキュリティ証明書がなければなりません。 この署名付き証明書は、証明書に署名した認証局（CA）のルート証明書とともに、各 OCS サーバにインストールする必要があります。

OCS サーバと IM and Presence サーバで同じ CA を共有することをお勧めします。 共有していない場合、IM and Presence 証明書に署名した CA のルート証明書も各 OCS サーバにインストールする必要があります。

通常、OCS CA のルート証明書は各 OCS サーバにすでにインストールされています。 したがって、OCS と IM and Presence が同じ CA を共有している場合、ルート証明書のインストールは必要ない場合があります。 ただし、ルート証明書が必要な場合は、次の詳細を参照してください。

Microsoft 認証局を使用している場合、Microsoft 認証局から OCS へのルート証明書のインストールについて、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』に記載の次の手順を参照してください。

- CA 証明書チェーンのダウンロード
- CA 証明書チェーンのインストール

代替 CA を使用している場合、次の手順が、ルート証明書を OCS サーバにインストールする一般的な手順になります。 CA からルート証明書をダウンロードする手順は、選択した CA によって異なります。

はじめる前に

CA からルート証明書または証明書チェーンをダウンロードし、OCS サーバのハード ディスクに保存します。

手順

ステップ 1 OCS サーバで、[開始（Start）] > [実行（Run）] を選択します。

ステップ 2 **mmc** と入力し、[OK] を選択します。

ステップ 3 [ファイル（File）] メニューで、[スナップインの追加と削除（Add/Remove Snap-in）] を選択します。

ステップ 4 [スナップインの追加と削除（Add/Remove Snap-In）] ダイアログボックスで、[追加（Add）] を選択します。

ステップ 5 [利用できるスタンドアロン スナップイン（Available Standalone Snap-ins）] リストで、[証明書（Certificates）] を選択し、[追加（Add）] を選択します。

ステップ 6 [コンピュータ アカウント（Computer Account）] を選択し、[次へ（Next）] を選択します。

ステップ 7 [コンピュータの選択（Select Computer）] ダイアログ ボックスで、[<ローカル コンピュータ>（このコンソールを実行しているコンピュータ）（Local Computer (the computer this console is running on)）] チェックボックスをオンにし、[終了（Finish）] を選択します。

ステップ 8 [閉じる（Close）] を選択し、続いて [OK] を選択します。

ステップ 9 [証明書（Certificates）] コンソールの左側のペインで、[証明書（ローカル コンピュータ）（Certificates (Local Computer)）] を展開します。

ステップ 10 [信頼されたルート証明機関（Trusted Root Certification Authorities）] を展開します。

ステップ 11 [証明書（Certificates）] を右クリックし、[すべてのタスク（All Tasks）] を選択します。

ステップ 12 [インポート（Import）] を選択します。

ステップ 13 インポート ウィザードで [次へ（Next）] を選択します。

ステップ 14 [参照（Browse）]を選択して、ルート証明書または証明書チェーンを保存した場所に移動します。

ステップ 15 ファイルを選択し、[開く（Open）] を選択します。

ステップ 16 [次へ（Next）] を選択します。

ステップ 17 [証明書をすべて次のストアに配置する（Place all certificates in the following store）] というデフォルト値のままにして、[証明書ストア（Certificate store）] の下に [信頼されたルート証明機関（Trusted Root Certification Authorities）] が表示されていることを確認します。

ステップ 18 [次へ（Next）] を選択し、続いて [終了（Finish）] を選択します。

ステップ 19 他の CA について、必要に応じて手順 11 ～ 18 を繰り返します。

（注） 『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』マニュアルでは、Access Edge サーバについて説明しています。 パーティション イントラドメイン フェデレーションについては、Access Edge サーバへの参照を OCS Standard Edition サーバまたは Enterprise Edition フロントエンド サーバと置き換えることができます。

次の作業

既存の OCS 署名付き証明書の検証, （64 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）
『Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager』

既存の OCS 署名付き証明書の検証

IM and Presence および OCS 間の TLS 暗号化をサポートするには、OCS サーバごとに、クライアント認証をサポートする署名付きセキュリティ証明書がなければなりません。 署名付き証明書がすでに OCS サーバにインストールされている場合、次の手順では、その既存の署名付き証明書がクライアント認証をサポートしているかどうか確認する方法について説明します。

（注）

- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンド サーバでこの手順を実行する必要があります。

手順

ステップ 1 OCS サーバで、[開始（Start）] > [実行（Run）] を選択します。

ステップ 2 **mmc** と入力し、[OK] を選択します。

ステップ 3 [ファイル（File）] メニューで、[スナップインの追加と削除（Add/Remove Snap-in）] を選択します。

ステップ 4 [スナップインの追加と削除（Add/Remove Snap-In）] ダイアログボックスで、[追加（Add）] を選択します。

ステップ 5 [利用できるスタンドアロン スナップイン（Available Standalone Snap-ins）] リストで、[証明書（Certificates）] を選択し、[追加（Add）] を選択します。

ステップ 6 [コンピュータ アカウント（Computer Account）] を選択し、[次へ（Next）] を選択します。

ステップ 7 [コンピュータの選択（Select Computer）] ダイアログ ボックスで、[<ローカル コンピュータ>（このコンソールを実行しているコンピュータ）（Local Computer (the computer this console is running on)）] チェックボックスをオンにし、[終了（Finish）] を選択します。

ステップ 8 [閉じる（Close）] を選択し、続いて [OK] を選択します。

ステップ 9 [証明書（Certificates）] コンソールの左側のペインで、[証明書（ローカル コンピュータ）（Certificates (Local Computer)）] を展開します。

ステップ 10 [個人（Personal）] を展開して、[証明書（Certificates）] を選択します。

ステップ 11 右側のペインで、現在 OCS により使用されている署名付き証明書を見つけます。

ステップ 12 [クライアント認証（Client Authentication）] が [使用目的（Intended Purposes）] カラムに記載されていることを確認します。

次の作業

認証局からの署名付き証明書の要求, （65 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

認証局からの署名付き証明書の要求

ここでは、次の手順について説明します。

- 署名付き証明書の OCS サーバへのインストール, （66 ページ）
- TLS ネゴシエーション用にインストールされた証明書の選択, （68 ページ）

（注） このトピックの手順は、OCS サーバに署名付き証明書が存在しない、または既存の証明書がクライアント認証をサポートしていない場合のみ必要です。

IM and Presence および OCS 間の TLS 暗号化をサポートするには、OCS サーバごとに、クライアント認証をサポートする署名付きセキュリティ証明書がなければなりません。 どの OCS サーバにも署名付きセキュリティ証明書がない場合、次の手順は、認証局から新たに署名した証明書を要求し、その特定の OCS サーバにインストールする方法の概要を説明します。

OCS からの証明書署名要求（CSR）で使用されている件名共通名（CN）は、OCS の展開により異なります。

- Standard Edition サーバの場合、Standard Edition サーバの FQDN を件名 CN として使用します。
- Enterprise Edition フロントエンド サーバの場合、フロントエンド サーバが属するプールの FQDN を件名 CN として使用します。

スタンドアロン Microsoft 認証局

スタンドアロン Microsoft 認証局を使用している場合、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』に記載の次の手順を参照して、OCS サーバの CA から署名付き証明書を要求します。

- CA サーバからの証明書の要求
- CA サーバからの証明書のダウンロード

（注） このマニュアルは Access Edge サーバについて説明しています。 パーティション イントラドメイン フェデレーションについては、Access Edge サーバへの参照を OCS Standard Edition サーバまたは Enterprise Edition フロントエンド サーバと置き換えることができます。

企業 Microsoft 認証局

企業 Microsoft 認証局を使用している場合、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』に記載の次の手順を参照して、CA で必要なテンプレートを生成し、OCS サーバの CA から署名付き証明書を要求します。

- 企業の認証局を使用した Access Edge のカスタム証明書の作成
- サイト サーバの署名付き証明書の要求

別の認証局

代替 CA を使用している場合、次の手順が、署名付き証明書を OCS サーバにインストールする一般的な手順になります。 署名付き証明書を要求する手順は、選択した CA によって異なります。

関連トピック

『Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager』

署名付き証明書の OCS サーバへのインストール

はじめる前に

CA から署名付き証明書をダウンロードし、OCS サーバのハード ディスクに保存します。

手順

ステップ 1 OCS サーバで、[開始（Start）] > [実行（Run）] を選択します。

ステップ 2 **mmc** と入力し、[OK] を選択します。

ステップ 3 [ファイル（File）] メニューで、[スナップインの追加と削除（Add/Remove Snap-in）] を選択します。

ステップ 4 [スナップインの追加と削除（Add/Remove Snap-In）] ダイアログボックスで、[追加（Add）] を選択します。

ステップ 5 [利用できるスタンドアロン スナップイン（Available Standalone Snap-ins）] リストで、[証明書（Certificates）] を選択し、[追加（Add）] を選択します。

ステップ 6 [コンピュータ アカウント（Computer Account）] を選択し、[次へ（Next）] を選択します。

ステップ 7 [コンピュータの選択（Select Computer）] ダイアログ ボックスで、[<ローカル コンピュータ>（このコンソールを実行しているコンピュータ）（Local Computer (the computer this console is running on)）] チェックボックスをオンにし、[終了（Finish）] を選択します。

ステップ 8 [閉じる（Close）] を選択し、続いて [OK] を選択します。

ステップ 9 [証明書（Certificates）] コンソールの左側のペインで、[証明書（ローカル コンピュータ）（Certificates (Local Computer)）] を展開します。

ステップ 10 [個人（Personal）] を展開します。

ステップ 11 [証明書（Certificates）] を右クリックし、[すべてのタスク（All Tasks）] を選択します。

ステップ 12 [インポート（Import）] を選択します。

ステップ 13 インポート ウィザードで [次へ（Next）] を選択します。

ステップ 14 [参照（Browse）] を選択して、署名付き証明書を保存した場所に移動します。

ステップ 15 ファイルを選択し、[開く（Open）] を選択します。

ステップ 16 [次へ（Next）] を選択します。

ステップ 17 [証明書をすべて次のストアに配置する（Place all certificates in the following store）] というデフォルト値のままにして、[証明書ストア（Certificate store）] の下に [個人（Personal）] が表示されていることを確認します。

ステップ 18 [次へ（Next）] を選択し、続いて [終了（Finish）] を選択します。

次の作業

TLS ネゴシエーション用にインストールされた証明書の選択, （68 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

TLS ネゴシエーション用にインストールされた証明書の選択

使用されている CA に関係なく、署名付き証明書が OCS サーバにインストールされたら、次の手順を実行して、TLS が IM and Presence とネゴシエーションする場合に OCS が使用するインストール済み証明書を選択する必要があります。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 Standard Edition サーバまたは Enterprise Edition フロントエンド サーバの FQDN を右クリックし、[プロパティ（Properties）] > [フロントエンドのプロパティ（Front End Properties）] を選択します。

ステップ 3 [セキュリティ（Security）] タブを選択し、[証明書の選択（Select Certificate）] を選択します。

ステップ 4 インストール済み証明書のリストから、新たに署名された証明書を選択し、[OK] を選択して [証明書の選択（Select Certificate）] ウィンドウを閉じます。

ステップ 5 [OK] を選択して [プロパティ（Properties）] ウィンドウを閉じます。

次の作業

OCS フロントエンド サーバでのサービスの再起動, （58 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

第 6 章

Microsoft Live Communications Server for Partitioned Intradomain Federation の設定

LCS サーバでポート 5060 を有効にする

IM and Presence と Microsoft Live Communications Server（LCS）との間の SIP トラフィックに暗号化されていない TCP 接続を使用したい場合は、LCS が TCP SIP ポート 5060 でリッスンするように設定する必要があります。 次の手順は、LCS サーバ上でポート 5060 を有効にする方法について説明します。

（注）

- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンドサーバでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（Programs）] > [管理ツール（Administrative Tools）] > [Live Communications Server 2005] を選択します。

ステップ 2 Standard Edition サーバまたは Enterprise Edition フロントエンド サーバの FQDN を右クリックし、[プロパティ（Properties）] をクリックします。

ステップ 3 [全般（General）] タブをクリックします。

ステップ 4 [接続（Connections）] にポート 5060 が記載されていない場合は、[追加（Add）] を選択します。

ステップ 5 [すべての利用可能な IP アドレス（All available IP Addresses）] を選択します。

ステップ 6 [トランスポート（Transport）] 値に **TCP** を選択します。

ステップ 7 [ポート（Port）] 値に **5060** を選択し、[OK] を選択して [接続の追加（Add Connection）] ウィンドウを閉じます。 これで、ポート 5060 が [接続（Connections）] リストに記載されているはずです。

ステップ 8 [OK] を選択して [プロパティ（Properties）] ウィンドウを閉じます。

次の作業

LCS スタティック ルートが IM and Presence をポイントするように設定, （70 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

LCS スタティック ルートが IM and Presence をポイントするように設定

LCS が IM and Presence に要求をルーティングできるようにするには、LCS サーバ上でスタティック ルートを設定する必要があります。 スタティック ルートは IM and Presence をポイントします。 次の手順は、必要なスタティック ルートを設定する方法を説明します。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのプールでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（Programs）] > [管理ツール（Administrative Tools）] > [Live Communications Server 2005] を選択します。

ステップ 2 必要に応じて、Enterprise Edition のプール名または Standard Edition のサーバ名を右クリックします。

ステップ 3 [プロパティ（Properties）] を選択します。

ステップ 4 [ルーティング（Routing）] タブを選択し、[追加（Add）] を選択します。

ステップ 5 [ユーザ値（User value）] に *****（アスタリスク）を入力します。

ステップ 6 たとえば、foo.com のように、IM and Presence サーバのドメインを入力します。

ステップ 7 [電話の URI（Phone URI）] チェックボックスがオフになっていることを確認します。

ステップ 8 FQDN を入力する場合は、[ネットワーク アドレス（Network Address）] を選択し、IM and Presence サーバの FQDN を入力します。 たとえば、cup1.foo.com などです。

ステップ 9 IP アドレスを入力する場合は、[IP アドレス（IP Address）] を選択し、IM and Presence サーバの IP アドレスを入力します。 たとえば、10.x.x.x などです。

ステップ 10 [トランスポート（Transport）] 値に **TCP** を選択します。

ステップ 11 [ポート（Port）] 値に **5060** と入力します。

ステップ 12 [要求 URI 内のホストを置き換える（Replace host in request URI）] チェックボックスがオフになっているのを確認し、[OK] を選択します。 新しいスタティック ルートがルーティング リストに表示されるはずです。

ステップ 13 [OK] を選択して [プロパティ（Properties）] ウィンドウを閉じます。

次の作業

LCS で IM and Presence 用のホスト認証を追加, （71 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

LCS で IM and Presence 用のホスト認証を追加

LCS が許可を求められることなく SIP 要求を IM and Presence から受け入れられるようにするには、IM and Presence サーバごとに LCS でホスト認証のエントリを設定する必要があります。

LCS と IM and Presence との間の TLS 暗号化を設定するのであれば、次のように、IM and Presence サーバごとに 2 つのホスト認証エントリを追加する必要があります。

- 最初のエントリには、IM and Presence サーバの FQDN が含まれている必要があります。
- 2 つ目のエントリには、IM and Presence サーバの IP アドレスが含まれている必要があります。

TLS 暗号化を設定しない場合は、IM and Presence サーバごとに 1 つのホスト認証エントリのみを追加します。 このホスト認証エントリには、IM and Presence サーバの IP アドレスが含まれている必要があります。

次の手順では、必要なホスト認証エントリを追加する方法について説明します。

（注）

- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのプールでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（Programs）] > [管理ツール（Administrative Tools）] > [Live Communications Server 2005] を選択します。

ステップ 2 必要に応じて、Enterprise Edition のプール名または Standard Edition のサーバ名を右クリックします。

ステップ 3 [プロパティ（Properties）] を選択します。

ステップ 4 [ホストの承認（Host Authorization）] タブを選択して、[追加（Add）] を選択します。

ステップ 5 FQDN を入力する場合は、[ネットワーク アドレス（Network Address）] を選択し、IM and Presence サーバの FQDN を入力します。 たとえば、cup1.foo.com などです。

ステップ 6 IP アドレスを入力する場合は、[IP アドレス（IP Address）] を選択し、IM and Presence サーバの IP アドレスを入力します。 たとえば、10.x.x.x などです。

ステップ 7 [送信のみ（Outbound Only）] チェックボックスがオフになっていることを確認します。

ステップ 8 [サーバとして帯域を制限する（Throttle as Server）] チェックボックスをオンにします。

ステップ 9 [認証済みとして扱う（Treat as Authenticated）] をオンにします。

ステップ 10 [OK] をクリックして、[承認済みホストの追加（Add Authorized Host）] ウィンドウを閉じます。

ステップ 11 IM and Presence サーバごとに手順 4 ～ 10 を繰り返します。

ステップ 12 すべてのホスト認証エントリを入力したら、[OK] を選択して [プロパティ（Properties）] ウィンドウを閉じます。

次の作業

LCS サーバでのサービスの再起動, （73 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

LCS サーバでのサービスの再起動

LCS ですべての設定手順を完了したら、LCS サービスを再起動し、設定が有効になるようにします。

（注）
- この手順は、あらかじめスケジュールされたメンテナンスの時間帯に実施することをお勧めします。
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンドサーバでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（Programs）] > [管理ツール（Administrative Tools）] > [Live Communications Server 2005] を選択します。

ステップ 2 Standard Edition サーバまたは Enterprise Edition フロントエンド サーバの FQDN を右クリックし、[停止（Stop）] をクリックします。

ステップ 3 サービスが停止したら、Standard Edition サーバまたは Enterprise Edition フロントエンド サーバの FQDN を右クリックし、[スタート（Start）] をクリックします。

関連トピック

統合のトラブルシューティング, （107 ページ）

TLS 暗号化の設定

IM and Presence と LCS との間で TLS 暗号化を設定するには、次の手順を完了する必要があります。

- 連邦情報処理標準コンプライアンスを LCS で有効にする, （74 ページ）
- LCS 上での相互 TLS 認証の設定, （75 ページ）
- LCS への認証局のルート証明書のインストール, （76 ページ）
- 既存の LCS 署名付き証明書の検証, （78 ページ）
- 認証局からの署名付き証明書の要求, （79 ページ）

TLS設定が完了したら、LCSサーバでサービスを再起動する必要があります。LCSサーバでのサービスの再起動, （73 ページ）を参照してください。

連邦情報処理標準コンプライアンスを LCS で有効にする

IM and Presence と LCS との間で TLS 暗号化をサポートするには、LCS サーバ上で TLSv1 を有効にする必要があります。 TLSv1 は連邦情報処理標準（FIPS）コンプライアンスの一環として Windows サーバに組み込まれています。 次の手順では、FIPS コンプライアンスを有効にする方法について説明しています。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンド サーバでこの手順を実行する必要があります。

手順

ステップ 1 LCS サーバで、[スタート（Start）] > [すべてのプログラム（Programs）] > [管理ツール（Administrative Tools）] > [ローカル セキュリティ ポリシー（Local Security Policy）] を選択します。

ステップ 2 コンソール ツリーから、[ローカル ポリシー（Local Policies）] を選択します。

ステップ 3 [セキュリティ オプション（Security Options）] を選択します。

ステップ 4 [システム暗号化：暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う（System Cryptography: Use FIPS Compliant algorithms for encryption, hashing and signing）] をダブルクリックします。

ステップ 5 セキュリティ設定を有効にします。

ステップ 6 [OK] を選択します。

ステップ 7 [ローカル セキュリティの設定（Local Security Setting）] ウィンドウを閉じます。

次の作業

LCS 上での相互 TLS 認証の設定, （75 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

LCS 上での相互 TLS 認証の設定

IM and Presence と LCS との間で TLS 暗号化を設定するには、LCS サーバ上で相互 TLS 認証用のポート 5061 を設定する必要があります。 次の手順では、相互 TLS 認証用にポート 5061 を設定する方法について説明します。

（注）
- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンド サーバでこの手順を実行する必要があります。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（Programs）] > [管理ツール（Administrative Tools）] > [Live Communications Server 2005] を選択します。

ステップ 2 Standard Edition サーバまたは Enterprise フロントエンド サーバの FQDN を右クリックし、[プロパティ（Properties）] をクリックします。

ステップ 3 [全般（General）] タブを選択します。

ステップ 4 ポート 5061 に関連付いたトランスポートが [相互 TLS（Mutual TLS）] の場合は、手順 8 に進みます。

ステップ 5 ポート 5061 に関連付いたトランスポートが [相互 TLS（Mutual TLS）] でない場合は、[編集（Edit）] を選択します。

ステップ 6 [リモート サーバの認証（相互 TLS）（Authenticate remote server (Mutual TLS)）] をオンにします。

ステップ 7 [OK] をクリックして、[接続の編集（Edit Connection）] ウィンドウを閉じます。 ポート 5061 に関連付いたトランスポートが [相互 TLS（Mutual TLS）] になります。

ステップ 8 [OK] を選択して [プロパティ（Properties）] ウィンドウを閉じます。

次の作業

LCS への認証局のルート証明書のインストール, （76 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

LCS への認証局のルート証明書のインストール

IM and Presence と LCS との間の TLS 暗号化をサポートするには、LCS サーバごとに署名付きセキュリティ証明書が存在する必要があります。 この署名付き証明書は、証明書に署名した認証局（CA）のルート証明書とともに、LCS サーバごとにインストールする必要があります。

シスコは、LCS および IM and Presence サーバが同じ CA を共有するように推奨します。 そうしないと、IM and Presence の証明書に署名した CA も LCS サーバごとにインストールする必要があります。

一般的に、LCS の CA ルート証明書は、LCS サーバごとにあらかじめインストールされています。したがって、LCS と IM and Presence とが同じ CA を共有する場合、ルート証明書をインストールする必要はありません。 ただし、ルート証明書が必要な場合は、次の詳細を参照してください。

Microsoft Certificate Authority を使用している場合、Microsoft Certificate Authority から LCS へのルート証明書のインストールについて、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』で説明されている次の手順を参照してください。

- CA 証明書チェーンのダウンロード
- CA 証明書チェーンのインストール

別の CA を使用する場合は、次の手順が LCS サーバにルート証明書をインストールするための一般的な手順です。 CA からルート証明書をダウンロードする手順は、選択した CA によって異なります。

はじめる前に

ルート証明書または署名チェーンを CA からダウンロードし、LCS サーバのハードディスクに保存します。

手順

ステップ 1 LCS サーバで、[スタート（Start）] > [ファイル名を指定して実行（Run）] を選択します。

ステップ 2 **mmc** と入力し、[OK] を選択します。

ステップ 3 [ファイル（File）] メニューで、[スナップインの追加と削除（Add/Remove Snap-in）] を選択します。

ステップ 4 [スナップインの追加と削除（Add/Remove Snap-In）] ダイアログボックスで、[追加（Add）] を選択します。

ステップ 5 [利用できるスタンドアロン スナップイン（Available Standalone Snap-ins）] リストで、[証明書（Certificates）] を選択し、[追加（Add）] を選択します。

ステップ 6 [コンピュータ アカウント（Computer Account）] を選択し、[次へ（Next）] を選択します。

ステップ 7 [コンピュータの選択（Select Computer）] ダイアログ ボックスで、[<ローカル コンピュータ>（このコンソールを実行しているコンピュータ）（Local Computer (the computer this console is running on)）] チェックボックスをオンにし、[終了（Finish）] を選択します。

ステップ 8 [閉じる（Close）] を選択し、続いて [OK] を選択します。

ステップ 9 [証明書（Certificates）] コンソールの左側のペインで、[証明書（ローカル コンピュータ）（Certificates (Local Computer)）] を展開します。

ステップ 10 [信頼されたルート証明機関（Trusted Root Certification Authorities）] を展開します。

ステップ 11 [証明書（Certificates）] を右クリックし、[すべてのタスク（All Tasks）] を選択します。

ステップ 12 [インポート（Import）] を選択します。

ステップ 13 インポート ウィザードで [次へ（Next）] を選択します。

ステップ 14 [参照（Browse）]を選択して、ルート証明書または証明書チェーンを保存した場所に移動します。

ステップ 15 ファイルを選択し、[開く（Open）] を選択します。

ステップ 16 [次へ（Next）] を選択します。

ステップ 17 [証明書をすべて次のストアに配置する（Place all certificates in the following store）] というデフォルト値のままにして、[証明書ストア（Certificate store）] の下に [信頼されたルート証明機関（Trusted Root Certification Authorities）] が表示されていることを確認します。

ステップ 18 [次へ（Next）] を選択し、続いて [終了（Finish）] を選択します。

ステップ 19 他の CA について、必要に応じて手順 11 ～ 18 を繰り返します。

（注） 『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』ドキュメントには、Access Edge Server について記載されています。 パーティション化されたイントラドメイン フェデレーションでは、Access Edge Server への参照を LCS Standard Edition サーバまたは Enterprise Edition フロントエンド サーバと交換できます。

次の作業

既存の LCS 署名付き証明書の検証, （78 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）
『Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager』

既存の LCS 署名付き証明書の検証

IM and Presence と LCS との間の TLS 暗号化をサポートするには、LCS サーバごとにクライアント認証をサポートする署名付きセキュリティ証明書が存在する必要があります。 署名付き証明書がすでに LCS サーバにインストールされている場合、次の手順では、既存の署名付き証明書がクライアント認証をサポートしているかどうかを確認する方法について説明します。

（注）

- Standard Edition の場合、すべての Standard Edition サーバでこの手順を実行する必要があります。
- Enterprise Edition の場合、すべてのフロントエンド サーバでこの手順を実行する必要があります。

手順

ステップ 1 LCS サーバで、[スタート（Start）] > [ファイル名を指定して実行（Run）] を選択します。

ステップ 2 **mmc** と入力し、[OK] を選択します。

ステップ 3 [ファイル（File）] メニューで、[スナップインの追加と削除（Add/Remove Snap-in）] を選択します。

ステップ 4 [スナップインの追加と削除（Add/Remove Snap-In）] ダイアログボックスで、[追加（Add）] を選択します。

ステップ 5 [利用できるスタンドアロン スナップイン（Available Standalone Snap-ins）] リストで、[証明書（Certificates）] を選択し、[追加（Add）] を選択します。

ステップ 6 [コンピュータ アカウント（Computer Account）] を選択し、[次へ（Next）] を選択します。

ステップ 7 [コンピュータの選択（Select Computer）] ダイアログ ボックスで、[<ローカル コンピュータ>（このコンソールを実行しているコンピュータ）（Local Computer (the computer this console is running on)）] チェックボックスをオンにし、[終了（Finish）] を選択します。

ステップ 8 [閉じる（Close）] を選択し、続いて [OK] を選択します。

ステップ 9 [証明書（Certificates）] コンソールの左側のペインで、[証明書（ローカル コンピュータ）（Certificates (Local Computer)）] を展開します。

ステップ 10 [個人（Personal）] を展開して、[証明書（Certificates）] を選択します。

ステップ 11 右側のペインで、現在 LCS で使用されている署名付き証明書を見つけます。

ステップ 12 [クライアント認証（Client Authentication）] が [使用目的（Intended Purposes）] カラムに記載されていることを確認します。

次の作業

認証局からの署名付き証明書の要求, （79 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

認証局からの署名付き証明書の要求

ここでは、次の手順について説明します。

- 署名付き証明書の LCS サーバへのインストール, （80 ページ）
- TLS ネゴシエーション用にインストールされた証明書の選択, （82 ページ）

（注） 署名付き証明書が LCS サーバに存在している、または既存の証明書がクライアント認証をサポートしていない場合にのみ、このセクションの手順が必要です。

IM and Presence と LCS との間の TLS 暗号化をサポートするには、LCS サーバごとにクライアント認証をサポートする署名付きセキュリティ証明書が存在する必要があります。いずれの LCS サーバにも証明書が存在しない場合は、認証局から新たに署名付き証明書を要求し、その特定の LCS サーバにインストールする方法について、次の手順によって説明されます。

LCS から証明書署名要求（CSR）の中で使用される件名共通名（CN）は、LCS の展開に応じて異なります。

- Standard Edition サーバの場合、Standard Edition サーバの FQDN を件名 CN として使用します。
- Enterprise Edition フロントエンド サーバの場合、フロントエンド サーバが属するプールの FQDN を件名 CN として使用します。

スタンドアロン Microsoft 認証局

スタンドアロン Microsoft 認証局を使用している場合、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』に記載の次の手順を参照して、LCS サーバの CA から署名付き証明書を要求します。

- CA サーバからの証明書の要求
- CA サーバからの証明書のダウンロード

（注） このマニュアルは Access Edge サーバについて説明しています。 パーティション化されたイントラドメイン フェデレーションでは、Access Edge Server への参照を LCS Standard Edition サーバまたは Enterprise Edition フロントエンド サーバと交換できます。

企業 Microsoft 認証局

企業 Microsoft 認証局を使用している場合、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』に記載の次の手順を参照して、CA で必要なテンプレートを生成し、LCS サーバの CA から署名付き証明書を要求します。

- 企業の認証局を使用した Access Edge のカスタム証明書の作成
- サイト サーバの署名付き証明書の要求

別の認証局

別の CA を使用する場合は、次の手順が LCS サーバに署名付き証明書をインストールするための一般的な手順です。 署名付き証明書を要求する手順は、選択した CA によって異なります。

関連トピック

『Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager』

署名付き証明書の LCS サーバへのインストール

はじめる前に

署名付き証明書を CA からダウンロードし、LCS サーバのハードディスクに保存します。

手順

ステップ 1 LCS サーバで、[スタート（Start）] > [ファイル名を指定して実行（Run）] を選択します。

ステップ 2 **mmc** と入力し、[OK] を選択します。

ステップ 3 [ファイル（File）] メニューで、[スナップインの追加と削除（Add/Remove Snap-in）] を選択します。

ステップ 4 [スナップインの追加と削除（Add/Remove Snap-In）] ダイアログボックスで、[追加（Add）] を選択します。

ステップ 5 [利用できるスタンドアロン スナップイン（Available Standalone Snap-ins）] リストで、[証明書（Certificates）] を選択し、[追加（Add）] を選択します。

ステップ 6 [コンピュータ アカウント（Computer Account）] を選択し、[次へ（Next）] を選択します。

ステップ 7 [コンピュータの選択（Select Computer）] ダイアログ ボックスで、[<ローカル コンピュータ>（このコンソールを実行しているコンピュータ）（Local Computer (the computer this console is running on)）] チェックボックスをオンにし、[終了（Finish）] を選択します。

ステップ 8 [閉じる（Close）] を選択し、続いて [OK] を選択します。

ステップ 9 [証明書（Certificates）] コンソールの左側のペインで、[証明書（ローカル コンピュータ）（Certificates (Local Computer)）] を展開します。

ステップ 10 [個人（Personal）] を展開します。

ステップ 11 [証明書（Certificates）] を右クリックし、[すべてのタスク（All Tasks）] を選択します。

ステップ 12 [インポート（Import）] を選択します。

ステップ 13 インポート ウィザードで [次へ（Next）] を選択します。

ステップ 14 [参照（Browse）] を選択して、署名付き証明書を保存した場所に移動します。

ステップ 15 ファイルを選択し、[開く（Open）] を選択します。

ステップ 16 [次へ（Next）] を選択します。

ステップ 17 [証明書をすべて次のストアに配置する（Place all certificates in the following store）] というデフォルト値のままにして、[証明書ストア（Certificate store）] の下に [個人（Personal）] が表示されていることを確認します。

ステップ 18 [次へ（Next）] を選択し、続いて [終了（Finish）] を選択します。

次の作業

TLS ネゴシエーション用にインストールされた証明書の選択, （82 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

TLS ネゴシエーション用にインストールされた証明書の選択

どの CA が使用されるかにかかわらず、署名付き証明書が LCS サーバにインストールされたら、次の手順を実行し、IM and Presence との TLS ネゴシエーションで LCS が使用する目的でインストールされた証明書を選択する必要があります。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（Programs）] > [管理ツール（Administrative Tools）] > [Live Communications Server 2005] を選択します。

ステップ 2 Standard Edition サーバまたは Enterprise Edition フロントエンド サーバの FQDN を右クリックし、[プロパティ（Properties）] をクリックします。

ステップ 3 [セキュリティ（Security）] タブを選択し、[証明書の選択（Select Certificate）] を選択します。

ステップ 4 インストール済み証明書のリストから、新たに署名された証明書を選択し、[OK] を選択して [証明書の選択（Select Certificate）] ウィンドウを閉じます。

ステップ 5 [OK] を選択して [プロパティ（Properties）] ウィンドウを閉じます。

次の作業

LCS サーバでのサービスの再起動, （73 ページ）

関連トピック

統合のトラブルシューティング, （107 ページ）

第 7 章

ユーザの移行

シスコのユーザ移行ツール

シスコでは、LCS/OCS から IM and Presence へのユーザの移行プロセスを支援するために、次のツールを提供しています。

- 連絡先リスト エクスポート ツール：ユーザの移行用に LCS/OCS から連絡先リストを一括でエクスポートすることができます。
- アカウント無効化ツール：移行するユーザの LCS/OCS アカウントを無効にできます。
- アカウント削除ツール：移行するユーザを LCS/OCS から削除することで、それらのユーザへのプレゼンス要求が後から IM and Presence にルーティングされるようにします。

これらのユーザ移行ツールは、cisco.com の IM and Presence ソフトウェア ダウンロード ページ（http://www.cisco.com/en/US/products/sw/voicesw/ps556/index.html）から、zip ファイルとしてまとめてダウンロードできます。

zip ファイルには、3 つのツールと version.txt という名前のテキスト ファイルが含まれています。テキスト ファイルには、ツールの現在のバージョン番号が含まれており、ツールと同じフォルダに保存する必要があります。 ツールが別のフォルダに保存されている場合は、それぞれの場所にテキスト ファイルのコピーを保存する必要があります。 テキスト ファイルが同じフォルダにないと、ツールの実行時にエラーが表示され、ツールが実行されません。

移行前の推奨事項

シスコでは、LCS/OCS から IM and Presence にユーザを移行する前に次のタスクを実行するのを推奨しています。

- 無制限の連絡先リストとウォッチャの設定
- サブスクリプション要求の自動許可の有効化

無制限の連絡先リストとウォッチャの設定

LCS/OCS から IM and Presence にユーザを移行する前に、IM and Presence に関する [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）] の設定を無制限に設定することをシスコでは推奨しています。 そうすることで、移行された各連絡先リストが IM and Presence に完全にインポートされます。

すべてのユーザが IM and Presence に移行されたら、IM and Presence に関する [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）] の設定を望ましい値にリセットしてください。 システムのデフォルト値は、[連絡先リストの最大サイズ（Maximum Contact List Size）] が 200 で、[ウォッチャの最大数（Maximum Watchers）] が 200 です。

次の手順では、[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）] の設定に無制限の値を設定する方法について説明します。

（注） マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。[プレゼンス（Presence）] の設定を変更すると、変更内容がクラスタ内のすべてのノードに適用されます。そのため、任意のクラスタ内の IM and Presence パブリッシャ ノードでのみ設定するようにしてください。

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 [最大連絡先サイズ（ユーザごと）（Maximum Contact List Size (per user)）] には、[無制限（No Limit）] オプションをオンにします。

ステップ 3 [ウォッチャの最大数（ユーザごと）（Maximum Watchers (per user)）] には、[無制限（No Limit）] オプションをオンにします。

ステップ 4 [保存（Save）] を選択します。

ステップ 5 クラスタ内のすべての IM and Presence ノード上で Cisco XCP ルータを再起動します。 Cisco XCP ルータを再起動するには、[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）] を選択します。

サブスクリプション要求の自動許可の有効化

移行中のユーザ エクスペリエンスを改善するために、シスコでは、移行プロセスを開始する前に、サブスクリプション要求の自動許可を許可することをお勧めします。 そうしないと、IM and Presence の各ユーザは、IM and Presence に連絡先としてインポートされるごとにサブスクリプション要求を手動で許可するように強制されます。 この設定は、必要に応じて、すべての移行が完了した後に無効にする必要があります。

次の手順は、サブスクリプション要求の自動許可を有効にする方法について説明します。

（注） この設定は、IM and Presence ではデフォルトで有効になっています。

（注） マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。[プレゼンス（Presence）] の設定を変更すると、変更内容がクラスタ内のすべてのノードに適用されます。そのため、任意のクラスタ内の IM and Presence パブリッシャ ノードでのみ設定するようにしてください。

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 [承認を要求されることなく、ユーザが他のユーザの空き状況を確認できるようにする（Allow users to view the availability of other users without being prompted for approval）] をオンにします。

ステップ 3 [保存（Save）] を選択します。

ステップ 4 クラスタ内のすべての IM and Presence ノード上で Cisco XCP ルータを再起動します。 Cisco XCP ルータを再起動するには、[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）] を選択します。

Cisco Unified Communications Manager 上での LCS/OCS ユーザのプロビジョニング

Microsoft Live Communications Server（LCS）または Microsoft Office Communications Server（OCS）から IM and Presence にユーザを移行する最初の手順としては、LCS/OCS Cisco Unified Communications Manager 上のユーザをプロビジョニングし、IM and Presence と IM and Presence がサポートするクライアントに対してそれらのユーザにライセンスを付与します。

Cisco Unified Communications Manager での新規ユーザの設定、および IM and Presence サービスと IM and Presence がサポートするクライアントのライセンス要件については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

関連項目

『Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager』

次の作業

ユーザ LCS/OCS の連絡先リスト情報のバックアップ, （86 ページ）

ユーザ LCS/OCS の連絡先リスト情報のバックアップ

LCS / OCS は dbimpexp.exe というツールを提供します。 シスコでは、後日、必要に応じて LCS/OCS に関する情報を復元できるように、このツールを使用して LCS/OCS のユーザ連絡先リストの情報をバックアップすることをお勧めします。

IM and Presence でサポートされているクライアントに LCS/OCS ユーザを移行するには、このツールを使用して個々の LCS/OCS ユーザまたはすべてのユーザの連絡先リストをバックアップできます。

関連項目

dbimpexp.exe ツールの使用方法：http://www.ocspedia.com/Misc/Explore_Dbimpexp.aspx?ArticleID=41

次の作業

ユーザを移行するための連絡先リストのエクスポート，（87 ページ）

ユーザを移行するための連絡先リストのエクスポート

シスコは、管理者がユーザを移行するために LCS/OCS 連絡先リストを一括でエクスポートできるように、連絡先リスト エクスポート ツール（ExportContacts.exe）を提供します。 このツールは、連絡先リストをエクスポートしてカンマ区切り値（CSV）ファイルに出力するのに、LCS/OCS アプリケーション プログラミング インターフェイス（API）を使用します。 その後、IM and Presence 一括管理ツール（BAT）がこのファイルを使用し、これらの同じ連絡先リストを移行時に後から IM and Presence にインポートできます。

（注）

- このツールは、サポートされているすべての LCS/OCS プラットフォームに対して実行できます。
- 任意の Standard Edition サーバまたは Enterprise Edition フロントエンド サーバで実行できます。
- このツールを実行しても、Microsoft Office Communicator にサインインしている他の LCS/OCS ユーザの能力には影響しません。 ただし、シスコでは、LCS/OCS および Active Directory システムへの負荷を減らすために、予定されたメンテナンス ウィンドウの中でこのツールを実行することをお勧めします。

このツールを実行すると、エクスポートした連絡先のリストを含むファイルが、ツールと同じディレクトリに作成されます。 ファイル名は ExportedContacts<Timestamp>.csv になります。 ファイルが作成されると、ファイル名にタイムスタンプが追加されるので、連絡先リスト エクスポート ツールを実行するたびに、一意の出力ファイルが作成されます。

また、連絡先リスト エクスポート ツールは、連絡先リストのエクスポート用に指定したユーザごとの LCS/OCS SIP URI を含む 2 番目のファイルも作成します。 ファイル名は、UserList<Timestamp>.txt で、これもツールと同じディレクトリに作成されます。

（注）

UserList<Timestamp>.txt ファイルを連絡先リスト エクスポート ツールおよびアカウント無効化ツールの入力データとして使用できます。

ログ ファイル

さらに連絡先リスト エクスポート ツールは、ツールを実行するたびに、出力ファイルと同じディレクトリ内に一意のタイムスタンプ付きのログ ファイルを作成します。 ログ ファイルのファイル名は ExportContactsLog<Timestamp>.txt になります。

連絡先リスト エクスポート ツールを実行するたびに、ログ ファイルをチェックすることをお勧めします。 その後、ログ ファイルをスキャンしてあらゆる問題を解決できます。 各ログ ファイルの一番下に、次の情報が要約されています。

- 正常に処理されたユーザ数
- 見つからなかったユーザ数
- エラーが原因で処理されなかったユーザ数
- 連絡先リストの最大サイズ
- 見つかった連絡先の数
- 連絡先リストの平均サイズ

実行モード

連絡先リスト エクスポート ツールには、NORMAL と STATSONLY という 2 つの実行モードがあります。 NORMAL は、ツールを実行する標準的な方法です。 このモードでは、エクスポートされた連絡先を含む CSV ファイル、ログ ファイル、およびユーザの LCS/OCS SIP URI ファイルという 3 つのファイルが作成されます。 STATSONLY モードでは、連絡先リスト エクスポート ツールはログ ファイルのみを作成します。 このモードでツールを実行すると、エクスポートされた連絡先の CSV ファイルと LCS/OCS SIP URI ファイルを作成する前に、エラーがあればそれを発見して修正することができます。

入力ファイルの形式

連絡先リスト エクスポート ツール（ExportContacts.exe）を使用すると、移行するユーザのリストを含む入力ファイルを指定できます。 その後、このツールが、入力ファイルで指定されたユーザの連絡先リストを取得します。 または、コマンドライン パラメータを指定することで、ローカル LCS/OCS データベース内のすべてのユーザの連絡先リストをエクスポートできます。

入力ファイルを使用する場合、次の入力ファイル形式がサポートされます。

入力ファイル形式 1：**LCS/OCS SIP URIs**

次の点に注意してください。

- 入力ファイルの各行は、連絡先リストの所有者を表します。
- 連絡先リストの所有者は、所有者の LCS/OCS SIP URI で表されます。たとえば、sip:bobjones@foo.com などです。
- 次のファイルは、サンプルの入力ファイルです。

```
sip:ann@foo.com sip:bob@foo.com sip:joe@foo.com sip:chuck@foo.com
```

入力ファイル形式 2：**IM and Presence ユーザ ID**

次の点に注意してください。

- IM and Presence BAT サブクラスタ エクスポート ツールを使用すると、この形式のファイルを取得できます。
- この形式は、カンマ区切り値（CSV）形式であり、入力ファイルの各行が連絡先リストの所有者に関するIM and Presence サブクラスタ割り当てデータを表します。
- 連絡先リストの所有者は、所有者の IM and Presence ユーザ ID で表されます。たとえば、bobjones などです。
- 次のファイルは、サンプルの入力ファイルです。ユーザ ID は太字になっています。

```
UserID,Subcluster Name,Node Name ann,CUPSubcluster1,CUPServer1
bob,CUPSubcluster1,CUPServer1 joe,CUPSubcluster1,CUPServer1
chuck,CUPSubcluster1,CUPServer1
```

  連絡先リスト エクスポート ツールは、Subcluster Name と Node Name の情報を無視し、ユーザ ID の値を使用します。

- このファイル形式を使用する場合は、ツールを実行する際に IM and Presence サーバのドメインを指定する必要があります。 ツールは、sip:userID@domain のようにドメインを使用して SIP URI をフォーマットします。

入力ファイル形式 3：Active Directory 内の組織別のユーザ

この入力ファイル形式では、移行するユーザが含まれる Active Directory 内の組織単位（OU）を指定できます。 入力ファイルには、次の形式である必要があります。

```
DN:OU=OrgUnit1,OU=OrgUnit2,DC=DomainComp1,DC=DomainComp2
```

ここで、OrgUnit1 は、OrgUnit2 OU 内の OU で、DomainComp1 と DomainComp2 はドメイン コンポートです。 ドメインには通常、たとえば cisco.com ドメインに対する cisco および com のように、AD 内の 2 つのドメイン コンポーネントが含まれます。

また、単一の入力ファイルに複数の識別名（DN）を指定して、別の OU のユーザの連絡先リストをエクスポートできます。 複数の DN が指定されている入力ファイルの形式は次のとおりです。

```
DN:OU=firstOU,DC=DomainComp1,DC=DomainComp2
DN:OU=secondOU,DC=DomainComp1,DC=DomainComp2
DN:OU=thirdOU,DC=DomainComp1,DC=DomainComp2
```

（注） 連絡先リスト エクスポート ツールが使用する入力ファイルのファイル名には、スペースや特殊文字を含めることはできません。

次の手順は、ユーザの移行用にLCS/OCSから連絡先リストを一括でエクスポートする方法について説明します。

手順

ステップ 1 Standard Edition サーバまたは Enterprise Edition フロントエンド サーバに、シスコのユーザ移行ツールを含む zip ファイルをコピーし、解凍します。

（注） 抽出した後、LCS/OCS サーバ上の別の場所にシスコのユーザ移行ツールのいずれかを移動した場合は、ツールが現在のバージョンを出力できるように新しい場所に version.txt ファイルもコピーする必要があります。

ステップ 2 コマンド プロンプトを開き、連絡先リスト エクスポート ツールのある場所にディレクトリを変更します。

ステップ 3 コマンド プロンプトで、次のようにツールを実行します。

目的	次のコマンドを入力
LCS/OCS SIP URI 入力ファイルで指定したように、ローカルデータベース内のユーザのリスト用の連絡先リストをエクスポートする **または** AD 入力ファイル内の組織単位別ユーザで指定したように、組織単位内のユーザのリスト用の連絡先リストをエクスポートする	`ExportContacts.exe -s/LDAPServer -f/input_file -l/logLevel -r/run_mode` 引数の説明 • `LDAPServer`：LCS/OCS ユーザが保存されている AD サーバの IP または FQDN • `input_file`：LCS/OCS SIP URI のリストを含むテキスト ファイル、または移行するユーザが含まれている AD の組織単位の識別名のリストを含むテキスト ファイル • `logLevel`：ロギング レベル。次のいずれかである必要があります。 ◦エラー ◦情報 ◦デバッグ（推奨） • `run_mode`：実行モード。次のいずれかである必要があります。 ◦NORMAL ◦STATSONLY

目的	次のコマンドを入力
IM and Presence ユーザ ID 入力ファイルで指定したように、ローカルデータベース内のユーザのリスト用の連絡先リストをエクスポートする	`ExportContacts.exe -s/LDAPServer -f/input_file -l/logLevel -d/Domain -r/run_mode` 引数の説明 • `LDAPServer`：LCS/OCS ユーザが保存されている AD サーバの IP または FQDN • `input_file`：IM and Presence ユーザ ID のリストを含むテキストファイル • `logLevel`：ロギング レベル。次のいずれかである必要があります。 ◦エラー ◦情報 ◦デバッグ（推奨） • `Domain`：IM and Presence サーバが存在するドメイン • `run_mode`：実行モード。次のいずれかである必要があります。 ◦NORMAL ◦STATSONLY
すべてのユーザの連絡先リストをエクスポートする	`ExportContacts.exe -s/LDAPServer -f/ALL -l/logLevel -r/run_mode` 引数の説明 • `LDAPServer`：LCS/OCS ユーザが保存されている AD サーバの IP または FQDN • `logLevel`：ロギング レベル。次のいずれかである必要があります。 ◦エラー ◦情報 ◦デバッグ（推奨） • `run_mode`：実行モード。次のいずれかである必要があります。 • NORMAL • STATSONLY

（注） 正しい連絡先リストが確実に移行されるようにするには、IM and Presence に連絡先リストをインポートする前に、エクスポートした連絡先リストの所有者を LCS/OCS 上で完全に無効にする必要があります。

次の作業

LCS/OCS でのユーザの無効化, （92 ページ）

関連トピック

連絡先リスト エクスポート ツール, （121 ページ）

LCS/OCS でのユーザの無効化

ここでは、次の手順について説明します。

- ユーザを移行するための LCS/OCS アカウントの無効化, （92 ページ）
- Active Directory の更新が LCS/OCS と同期していることの確認, （94 ページ）

ユーザを移行するための LCS/OCS アカウントの無効化

シスコでは、移行するユーザの LCS/OCS アカウントを無効にするツールを提供しています。 このツール（DisableAccount.exe）は、Active Directory（AD）に接続し、ユーザの LCS/OCS 属性を更新して LCS/OCS アカウントを無効にします。 アカウント無効化ツールの実行は、LCS/OCS でユーザの移行を無効にするために行われなければならない、次の2段階のプロセスの最初のステップです。

1 ユーザを移行するための LCS/OCS アカウントの無効化
2 ユーザを移行するための LCS/OCS ユーザ データの削除

（注）

- このツールは、サポートされているすべての LCS/OCS プラットフォームで実行できます。
- 任意の Standard Edition サーバまたは Enterprise Edition フロントエンド サーバでこのツールを実行できます。
- このツールを実行しても、Microsoft Office Communicator にサインインしている他の LCS/OCS ユーザの能力には影響しません。 ただし、シスコでは、LCS/OCS および Active Directory システムへの負荷を減らすために、予定されたメンテナンス ウィンドウの中でこのツールを実行することをお勧めします。

アカウント無効化ツールは、次のように 3 つの入力を受け付けます。

- LCS/OCS ユーザが存在する AD サーバの IP または FQDN
- 無効にする LCS/OCS ユーザ アカウントのリストを含む入力ファイル
- エラー、情報、またはデバッグのいずれかでなければならないロギング レベル（デバッグが推奨設定）

アカウント無効化ツールは、入力ファイルから無効にするユーザのリストを読み込みます。 入力ファイルの各行は、連絡先リストの所有者を表します。 連絡先リストの所有者は、所有者の LCS/OCS SIP URI で表されます。たとえば、sip:bobjones@cisco.com などです。 次のファイルは、サンプルの入力ファイルです。

```
sip:ann@cisco.com sip:bob@cisco.com sip:joe@cisco.com sip@chuck@cisco.com
```

上記の形式に基づいて、独自の入力ファイルを作成することができます。 ただし、シスコでは、ファイル無効化ツールの入力ファイルとして、UserList<Timestamp>.txt ファイルを使用することをお勧めします。 UserList<Timestamp>.txt ファイルには、重複したユーザ、無効なユーザ、または存在しないユーザは含まれません。

（注） アカウント無効化ツールが使用する入力ファイルのファイル名には、スペースや特殊文字を含めることはできません。

アカウント無効化ツールを実行すると、DisableAccountLog<Timestamp>.txt と呼ばれる一意のタイムスタンプが付加されたログファイルがツールと同じディレクトリに生成されます。 ログファイルには、発生した障害やエラーに関する詳細が含まれています。

はじめる前に

このツールを実行するには、AD に対する読み取り/書き込み権限が必要です。

手順

ステップ 1 Standard Edition サーバまたは Enterprise Edition フロントエンド サーバに、シスコのユーザ移行ツールを含む zip ファイルをコピーし、解凍します。

（注） 抽出した後、LCS/OCS サーバ上の別の場所にシスコのユーザ移行ツールのいずれかを移動した場合は、ツールが現在のバージョンを出力できるように新しい場所に version.txt ファイルもコピーする必要があります。

ステップ 2 コマンド プロンプトを開き、アカウント無効化ツールのある場所にディレクトリを変更します。

ステップ 3 コマンド プロンプトで、次のコマンドを入力します。

```
DisableAccount.exe -s/LDAPServer -f/input_file -l/logLevel
```

引数の説明

- `LDAPServer`：ユーザが存在する AD サーバの IP または FQDN

- `input_file`：無効にする LCS/OCS ユーザ アカウントのリストを含むファイルである UserList<Timestamp>.txt
- `logLevel`：エラー、情報、またはデバッグのいずれかでなければならないロギング レベル（デバッグが推奨設定）

ステップ 4 アカウント無効化ツールを実行した後は、毎回、DisableAccountLog<Timestamp>.txt ログ ファイルをチェックし、すべてのユーザが正常に無効になったかを確認します。

次の作業

Active Directory の更新が LCS/OCS と同期していることの確認, （94 ページ）

Active Directory の更新が LCS/OCS と同期していることの確認

LCS/OCS アカウントを無効にするために Active Directory の更新が行われると、次のステップでは、LCS/OCS にそれらの更新が同期されたかを確認します。 検証は、無効化された LCS/OCS アカウントがプロビジョニングされた Standard Edition サーバまたは Enterprise Edition プールで実行されます。

（注） LCS/OCS の配置に応じて、それらの変更が LCS/OCS に同期されるまでに最大 30 分かかります。

手順

ステップ 1 配置に応じて、次のいずれかを実行します。

- LCS 2005 を使用している場合、[スタート（Start）] > [すべてのプログラム（Programs）] > [管理ツール（Administrative Tools）] > [Live Communications Server 2005] を選択します。
- OCS 2007 R2 を使用している場合、[スタート（Start）] > [すべてのプログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 [ユーザ（Users）] を選択し、無効化したユーザが有効な LCS/OCS ユーザリストに表示されなくなったことを確認します。

次の作業

ユーザを移行するためのデータベースからのユーザ データの削除, （95 ページ）

関連トピック

アカウント無効化ツール，（122 ページ）

ユーザを移行するためのデータベースからのユーザデータの削除

（注） ユーザを移行するために LCS/OCS データベースからユーザデータを削除するには、LCS/OCS データベースへの読み取り/書き込み権限を持っている必要があります。

LCS/OCS は、LCS/OCS データベースからユーザを削除するための管理方法を提供します。 ただし、この方法でデータベースからユーザを削除すると、他のユーザの連絡先リストからそのユーザが削除されます。 シスコは、他の Microsoft Office Communicator ユーザの連絡先リストからユーザが削除されないようにするために、LCS/OCS データベースからユーザを削除する代替手段を提供しています。

この代替ツール（DeleteAccount.exe）を使用すると、移行するユーザを削除することで、それらのユーザへのプレゼンス要求が後から IM and Presence にルーティングされるようにします。 また、このツールは、削除されたユーザが LCS/OCS に残っているユーザの連絡先リストから削除されないようにします。 アカウント削除ツールの実行は、LCS/OCS でユーザの移行を無効にするための次の 2 段階のプロセスの 2 番目のステップです。 2 段階のプロセスは次のとおりです。

1. ユーザを移行するための LCS/OCS アカウントの無効化
2. ユーザを移行するための LCS/OCS ユーザ データの削除

（注）
- このツールは、サポートされているすべての LCS/OCS プラットフォームで実行できます。
- 任意の Standard Edition サーバまたは Enterprise Edition プールでこのツールを実行できます。
- このツールを実行しても、Microsoft Office Communicator にサインインしている他の LCS/OCS ユーザの能力には影響しません。 ただし、シスコでは、LCS/OCS および Active Directory システムへの負荷を減らすために、予定されたメンテナンス ウィンドウの中でこのツールを実行することをお勧めします。

アカウント削除ツールは、入力ファイルから削除するユーザのリストを読み込みます。 入力ファイルの各行は、連絡先リストの所有者を表します。 連絡先リストの所有者は、所有者の LCS/OCS SIP URI で表されます。たとえば、sip:bobjones@cisco.com などです。 次のファイルは、サンプルの入力ファイルです。

```
sip:ann@cisco.com sip:bob@cisco.com sip:joe@cisco.com sip@chuck@cisco.com
```

上記の形式に基づいて、独自の入力ファイルを作成することができます。 ただし、シスコでは、ファイル削除ツールの入力ファイルとして、UserList<Timestamp>.txt ファイルを使用することをお勧めします。 UserList<Timestamp>.txt ファイルには、重複したユーザ、無効なユーザ、または存在しないユーザは含まれません。

（注） アカウント削除ツールが使用する入力ファイルのファイル名には、スペースや特殊文字を含めることはできません。

Standard Edition の配置環境でのアカウント削除ツールの実行

ユーザのリストのデータを削除する際には、各 Standard Edition サーバで一度このツールを実行する必要があります。 データベースは、Standard Edition サーバ上で混在します。

Enterprise Edition の配置環境でのアカウント削除ツールの実行

ユーザのリストのデータを削除する際には、各 Enterprise Edition プールで一度このツールを実行する必要があります。 ツールは、任意のフロントエンド サーバまたはバックエンド データベース サーバ上で実行できます。 LCS/OCS フロントエンドが接続する LCS SQL サーバ名または OCS データベース インスタンス名が両方のオプションで指定されている必要があります。

手順

ステップ 1 このツールを実行する前に、LCS/OCSデータベースへの読み取り/書き込み権限があることを確認します。

ステップ 2 Standard Edition サーバまたは Enterprise Edition プール サーバ（フロントエンドまたはバックエンド）の 1 つに、シスコのユーザ移行ツールを含む zip ファイルをコピーし、解凍します。

（注） 抽出した後、LCS/OCS サーバ上の別の場所にシスコのユーザ移行ツールのいずれかを移動した場合は、ツールが現在のバージョンを出力できるように新しい場所に version.txt ファイルもコピーする必要があります。

ステップ 3 コマンド プロンプトを開き、アカウント削除ツールのある場所にディレクトリを変更します。

ステップ 4 コマンド プロンプトで、次のようにコマンドを入力します。

```
DeleteAccount.exe -s/database_instance -f/input_file -l/logLevel
```

引数の説明

- `database_instance`：OCS プールのデータベース インスタンス名または LCS プールの SQL サーバ インスタンス
- `input_file`：削除する LCS/OCS ユーザ アカウントのリストを含むファイルである UserList<Timestamp>.txt
- `logLevel`：エラー、情報、またはデバッグのいずれかでなければならないロギング レベル（デバッグが推奨設定）

ステップ 5 Standard Edition サーバまたは Enterprise Edition プールごとに、手順 1 ～ 3 を繰り返します。

トラブルシューティングのヒントについては、アカウント削除ツール，（123 ページ）を参照してください。

コマンドを実行すると、アカウント削除ツールによって DeleteAccountLog<Timestamp>.txt と呼ばれる一意のタイムスタンプが付加されたログ ファイルがツールと同じディレクトリに生成されます。 ログファイルには、発生した障害やエラーに関する詳細が含まれています。

次の作業

IM and Presence にユーザを移行するための連絡先リストのインポート，（97 ページ）

IM and Presence にユーザを移行するための連絡先リストのインポート

IM and Presence 一括管理ツール（BAT）を使用して LCS/OCS ユーザ連絡先リストを IM and Presence にインポートします。

次の手順を完了し、LCS/OCS ユーザ連絡先リストを IM and Presence にインポートします。

1. BAT を使用して CSV ファイルをアップロードします。
2. 新しい一括管理ジョブを作成します。
3. 一括管理ジョブの結果を確認します。

（注） デフォルトの連絡先リストのインポート速度は、サーバ 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 サービス（Cisco Bulk Provisioning Service）] を選択して連絡先リストのインポート速度を変更できます。 ただし、デフォルトのインポート速度を上げると、IM and Presence の CPU とメモリの使用率が増加します。

はじめる前に

LCS/OCS ユーザの連絡先リストをインポートする手順は、ユーザ移行プロセスの最後のステップの 1 つです。 LCS/OCS ユーザ連絡先リストをインポートする前に、以下の手順を完了する必要があります。

1. Cisco Unified Communications Manager 上で LCS/OCS ユーザをプロビジョニングします。
2. LCS/OCS ユーザがライセンスを取得し、IM and Presence に割り当てられていることを確認します。
3. すべての連絡先リストが完全にインポートされるように、IM and Presence の [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

定が無制限に設定されていることを確認します。 無制限の連絡先リストとウォッチャの設定, （84 ページ）を参照してください。

4 連絡先リストエクスポートツールを実行し、ExportedContacts<Timestamp>.csv ファイルを生成します。 ユーザを移行するための連絡先リストのエクスポート, （87 ページ）を参照してください。

5 LCS/OCS ユーザが LCS/OCS で完全に無効になっていることを確認します。 LCS/OCS でのユーザの無効化, （92 ページ）を参照してください。

BAT を使用した CSV ファイルのアップロード

ExportedContacts<Timestamp>.csv ファイルを BAT を使用して IM and Presence にアップロードする必要があります。 CSV ファイルのアップロード方法に関する手順については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

関連項目

『Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager』

次の作業

新しい一括管理ジョブの作成, （98 ページ）

新しい一括管理ジョブの作成

CSV ファイルをアップロードしたら、Cisco Unified CM IM and Presence の管理の中で新しい一括管理ジョブを作成し、ユーザ連絡先リストを更新する必要があります。 新しい一括管理ジョブの作成方法に関する手順については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

関連項目

『Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager』

次の作業

一括管理ジョブの結果, （98 ページ）

一括管理ジョブの結果

一括管理ジョブが完了すると、IM and Presence 一括管理ツールは、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。 一括管理ジョブの結果の確認方法に関する手順については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

次の作業

ユーザ デスクトップへの IM and Presence でサポートされているクライアントの導入, （99 ページ）

関連トピック

『Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager』
ユーザ移行のトラブルシューティング, （120 ページ）

ユーザ デスクトップへの IM and Presence でサポートされているクライアントの導入

LCS/OCS ユーザを Cisco Jabber にプロビジョニングし、IM and Presence と IM and Presence でサポートされているクライアントのライセンスを付与したら、ユーザデスクトップ上にクライアントソフトウェアをインストールできます。 IM and Presence でサポートされているクライアントの導入については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

関連トピック

『Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager』

連絡先リストと最大ウォッチャの最大サイズのリセット

LCS/OCS から IM and Presence にユーザを移行する前に、IM and Presence に関する [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）] の設定を無制限に設定することをシスコでは推奨しています。 そうすることで、移行された各連絡先リストが IM and Presence に完全にインポートされます。

すべてのユーザが IM and Presence に移行されたら、IM and Presence に関する [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）] の設定を望ましい値にリセットしてください。 システムのデフォルト値は、[連絡先リストの最大サイズ（Maximum Contact List Size）] が 200 で、[ウォッチャの最大数（Maximum Watchers）] が 200 です。

（注） LCS/OCS から IM and Presence にユーザを段階的に移行している場合は、すべてのユーザが移行されるまで、[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）] の値をリセットしないでください。

次の手順では、[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）] の設定に値を指定する方法について説明します。

（注） マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。[プレゼンス（Presence）] の設定を変更すると、変更内容がクラスタ内のすべてのノードに適用されます。そのため、任意のクラスタ内の IM and Presence パブリッシャ ノードでのみ設定するようにしてください。

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 [最大連絡先サイズ（ユーザごと）（Maximum Contact List Size (per user)）] には、[無制限（No Limit）] オプションをオフにし、希望する制限値を入力します。

ステップ 3 [ウォッチャの最大数（ユーザごと）（Maximum Watchers (per user)）] には、[無制限（No Limit）] オプションをオフにし、希望する制限値を入力します。

ステップ 4 [保存（Save）] を選択します。

ステップ 5 クラスタ内のすべての IM and Presence ノード上で Cisco XCP ルータを再起動します。 Cisco XCP ルータを再起動するには、[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）] を選択します。

第 8 章

IM and Presence のドメイン内 LCS/OCS のドメイン間フェデレーション機能との統合

Microsoft LCS/OCS は、リモート企業またはパブリック IM プロバイダーとのドメイン間フェデレーションをサポートしています。 このイントラドメイン フェデレーション機能は、LCS/OCS および IM and Presence 間でパーティション イントラドメイン フェデレーションが設定されている場合、Microsoft Office Communicator ユーザも使用できます。

さらに、IM and Presence 対応クライアントに移行するユーザが LCS/OCS で設定されたドメイン間フェデレーション機能を使用できるよう、IM and Presence を設定できます。

この章では、IM and Presence を LCS/OCS ドメイン間フェデレーション機能と統合する手順について説明します。

LCS/OCS とのパーティション イントラドメイン フェデレーションが有効な場合、SIP 対応および XMPP 対応両方のイントラドメイン フェデレーションを IM and Presence のリモート ドメインに設定することもできます。 ただし、このフェデレーション機能は IM and Presence 対応クライアントのユーザのみ使用できます。 IM and Presence でのドメイン間フェデレーションの設定方法の詳細については、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』（http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_installation_and_configuration_guides_list.html）を参照してください。

- リモート ドメインの SIP フェデレーション ドメインとしての設定，101 ページ
- リモート ドメインのスタティック ルートの設定，102 ページ
- LCS/OCS ドメイン間フェデレーション機能と IM and Presence との統合の削除，104 ページ

リモート ドメインの SIP フェデレーション ドメインとしての設定

リモート ドメインへのすべての要求は、IM and Presence と LCS/OCS との間で SIP インターフェイスを介してルーティングされるため、まず、IM and Presence 上で LCS/OCS SIP フェデレーショ

ン ドメインとしてリモート ドメインを設定する必要があります。 この手順は、リモート ドメインごとに実行する必要があります。

SIP フェデレーション ドメインの設定方法に関する手順については、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』の「Adding a SIP Federated Domain procedure」を参照してください。 SIP フェデレーション ドメインを設定する場合は、次のオプションを選択します。

- [ドメイン名（Domain Name）] には、リモート ドメインを入力します。
- [統合タイプ（Integration Type）] には、[ドメイン間から OCS（Inter-domain to OCS）] を選択します。
- [ダイレクト フェデレーション（Direct Federation）] がオンになっていることを確認します。

（注） マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。これらの設定はクラスタ全体で有効になります。したがって、ある指定のクラスタ内の IM and Presence パブリッシャ ノードでのみ設定する必要があります。

次の作業

リモート ドメインのスタティック ルートの設定, （102 ページ）

関連トピック

『Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager』統合のトラブルシューティング, （107 ページ）

リモート ドメインのスタティック ルートの設定

IM and Presence を LCS/OCS ドメイン間フェデレーション機能と統合する場合、リモート ドメインごとに IM and Presence 上にスタティック ルートを設定する必要があります。

Standard Edition LCS/OCS の場合、スタティック ルートは特定の Standard Edition サーバの IP アドレスを指す必要があります。

Enterprise Edition LCS/OCS の場合、スタティック ルートは特定の Enterprise Edition フロントエンド サーバまたはフロントエンド ロード バランサ（LCS/OCS フロントエンド ロード バランサを通じてルーティングする場合）を指す必要があります。

LCS/OCS フロントエンド ロードバランサを使用している場合は、次の点に注意してください。

- IM and Presence は、LCS/OCS フロントエンド ロード バランサとして Cisco Application Control Engine（ACE）を使用してテストされています。
- 他のロード バランサを ACE の代わりに使用できます。他のロード バランサのリストについては、次の URL を参照してください。http://technet.microsoft.com/en-us/office/ocs/cc843611 ただし、それらのロード バランサを導入し、正しく管理するのはお客様の責任です。 シスコ

では、そのようなロード バランサを指すようなスタティック ルートの構成をサポートしていません。

- ACE が設定されたフロントエンドのロード バランサでないような導入環境では、フロントエンド ロードバランサをバイパスするためのスタティック ルートを設定することをお勧めします。

ハイ アベイラビリティのためには、追加のバックアップ スタティック ルートをリモート ドメインごとに設定できます。 バックアップ ルートの優先順位は低く、プライマリ スタティック ルートの次のホップ アドレスに到達できない場合にのみ使用されます。

（注） マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。これらの設定はクラスタ全体で有効になります。したがって、ある指定のクラスタ内の IM and Presence パブリッシャ ノードでのみ設定する必要があります。

手順

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

ステップ 3 ドメイン、つまり FQDN が元に戻るよう [宛先パターン（Destination Pattern）] 値を入力します。たとえば、ドメインが remote.com である場合、宛先パターンの値 com.remote にならなければなりません。

ステップ 4 [ルート タイプ（Route Type）] で [ドメイン（domain）] を選択します。

ステップ 5 [ネクスト ホップ（Next Hop）] フィールドに次のホップの IP アドレスを入力します。

ステップ 6 [ネクスト ホップ ポート（Next Hop Port）] および [プロトコル タイプ（Protocol Type）] を次のように設定します。

- TLS 暗号化の場合：
  - [ネクスト ホップ ポート（Next Hop Port）] の番号は **5061**
  - [プロトコル タイプ（Protocol Type）] は、**TLS**
- TCP の場合：
  - [ネクスト ホップ ポート（Next Hop Port）] の番号は **5060**
  - [プロトコル タイプ（Protocol Type）] は、**TCP**

ステップ 7 [プライオリティ（Priority）] 値を次のように入力します。

- プライマリ スタティック ルートについては、デフォルトの [プライオリティ（Priority）] 値 **1** を入力します。
- バックアップ スタティック ルートについては、1 より大きい [プライオリティ（Priority）] 値を入力します （値が低いほど、スタティック ルートの優先度が高くなります）。

ステップ 8 他のすべてのパラメータにはデフォルト値を選択します。

ステップ 9 [保存（Save）] を選択します。

関連トピック

統合のトラブルシューティング, （107 ページ）

LCS/OCS ドメイン間フェデレーション機能と IM and Presence との統合の削除

ある段階で、LCS/OCS 上で以前設定したリモート ドメインの 1 つを使用して、ドメイン間フェデレーションの IM and Presence を設定したい場合があります。 これに関して最も可能性の高いシナリオとしては、すべてのMicrosoft Office Communicator ユーザが IM and Presence に移行された場合などが考えられます。 この時点で、LCS/OCS の展開をシャットダウンし、すべてのドメイン間フェデレーション機能は、代わりに IM and Presence から直接有効にできます。

LCS/OCS ドメイン間フェデレーション機能と IM and Presence との統合を削除するには、次の手順を完了する必要があります。

- リモート ドメインへのスタティック ルートの削除
- すべての SIP フェデレーション ドメインの削除

リモート ドメイン用のスタティック ルートの削除

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）] > [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 表示されるリストから適切なスタティック ルートを選択します。 リストが表示されない場合、[検索（Find）] を選択します。

ステップ 3 [選択項目の削除（Delete Selected）] を選択します。

ステップ 4 [OK] を選択して削除を確認します。

次の作業

SIP フェデレーション ドメインの削除, （105 ページ）

SIP フェデレーション ドメインの削除

（注） マルチクラスタを導入している場合は、各クラスタで、この手順を実行する必要があります。これらの設定はクラスタ全体で有効になります。したがって、ある指定のクラスタ内の IM and Presence パブリッシャ ノードでのみ設定する必要があります。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [ドメイン間フェデレーション（Inter-Domain Federation）] > [SIP フェデレーション（SIP Federation）] を選択します。

ステップ 2 表示されるリストからドメインを選択します。 リストが表示されない場合、[検索（Find）] を選択します。

ステップ 3 [選択項目の削除（Delete Selected）] を選択します。

ステップ 4 [OK] を選択して削除を確認します。

次の作業

リモート ドメインへのスタティック ルートを削除し、SIP フェデレーション ドメインを削除したら、リモート ドメインを使用してドメイン間フェデレーション用の IM and Presence の設定に進むことができます。 詳細については、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

第 9 章

統合のトラブルシューティング

IM and Presence のトレース

IM and Presence サーバ上では、SIP Proxy が SIP 要求のルーティングを担当し、XCP SIP Federation Connection Manager は、Microsoft SIP とネイティブ XMPP 間の SIP プロトコル変換を担当します。そのため、これらのサービスは、IM and Presence と Microsoft Live Communications Server（LCS）または Microsoft Office Communications Server（OCS）との間の SIP のパーティション化されたイントラドメイン フェデレーション統合の中核を成します。

XCP ルータは、IM and Presence の中核サービスです。 これは、要求の受信者が LCS/OCS ユーザまたは IM and Presence ユーザのいずれであるかを決定します。

ログファイルの場所は次のとおりです。

- XCP SIP Federation Connection Manager のログ：/var/log/active/epas/trace/xcp/log/sip-cm-3_000*.log
- SIP Proxy のログ：/var/log/active/epas/trace/esp/sdi/esp000*.log
- XCP Router のログ：var/log/active/epas/trace/xcp/log/rtr-jsm-1_000*.log

SIP Proxy のログの例

```
2:26:18.719 |PID(25333) sip_protocol.c(5964) Received 536 bytes TCP packet
 from 10.53.56.17:34282SUBSCRIBE sip:ysam@cuplcs.net SIP/2.0^M From:
<sip:fbear@cuplcs.net>;tag=a4cdaec0-1138350a-13d8-45026-4d755b8a-2162aa7a-4d755b8a^M
 To: <sip:ysam@cuplcs.net>^M Call-ID:
a30386f0-1138350a-13d8-45026-4d755b8a-2c25871c-4d755b8a^M CSeq: 1
SUBSCRIBE^M Via: SIP/2.0/TCP
10.53.56.17:5080;branch=z9hG4bK-4d755b8a-926d95b4-3c330144^M Expires:
```

```
7446^M Accept: application/pidf+xml, application/cpim-pidf+xml^M
User-Agent: Cisco-Systems-Partitioned 8.0^M Max-Forwards: 70^M Event:
presence^M Contact: <sip:10.53.56.17:5080;transport=TCP>^M Content-Length:
 0^M … 22:26:18.719 |ID(25333) sip_sm.c(4977) SIPGW Partitioned Fed UA
Header found in this request 22:26:18.719 |ID(25333) sip_sm.c(5010) This
 is a partitioned federation request, skip User Location DB lookup
22:26:18.719 |ID(25333) sip_sm.c(5200) This is an outbound Partitioned
federation request. 22:26:18.719 |Mon Mar 07 22:26:18 2011] PID(25333)
mod_sip_routing.c(1435) Routing: dipping for cuplcs.net 22:26:18.719 |Mon
 Mar 07 22:26:18 2011] PID(25333) mod_sip_routing.c(1473) Routing: Found
 domain route for cuplcs.net:10.53.56.18:5061;TLS pwf 1:1:5 22:26:18.719
 |ID(25333) sip_dns.c(811) "A" Query for 10.53.56.18 successful, Got 1
IP addresses 22:26:18.719 |ID(25333) sip_dns.c(139) A Record : 10.53.56.18
```

SIP Federation Connection Manager のログの例

次の例は、発信要求ログから抽出したものです。

```
21:48:44.277 |SIPGWDir.cpp:463: [FROM XMPP] <presence
from='fbear@cuplcs.net' to='ysam@cuplcs.net' type='probe'/>... ...
21:48:44.743 |SIPGWController.cpp:622: Skipping DNS lookup: <presence
from='fbear@cuplcs.net' to='ysam@cuplcs.net' type='probe'/> 21:48:44.743
 |SIPGWController.cpp:704: Entering _handleOutContinue: <presence
from='fbear@cuplcs.net' to='ysam@cuplcs.net' type='probe'/> 21:48:44.743
 |SIPGWController.cpp:989: _findSession (JID): local(fbear@cuplcs.net)
remote(ysam@cuplcs.net) 21:48:44.743 |SIPGWController.cpp:999:
_findSession: Session not found 21:48:44.743 |SIPHostInfo.cpp:82:
hostinfo(0x09a10ce8) refInc: 3 cuplcs.net:cuplcs.net 21:48:44.743
|SIPGWSession.cpp:58: Creating SIPGWSession sess=0x09a5a090
local=fbear@cuplcs.net remote=ysam@cuplcs.net 21:48:44.743
|SIPGWController.cpp:1017: _findSession: Made new session: sess=0x09a5a090
 local(fbear@cuplcs.net) remote(ysam@cuplcs.net) 21:48:44.743
|SIPGWSession.cpp:990: sess=0x09a5a090 Entering handleOut: <presence
from='fbear@cuplcs.net' to='ysam@cuplcs.net' type='probe'/> 21:48:44.743
 |SIPGWSession.cpp:1090: _createOutgoingSubs local=fbear@cuplcs.net,
remote=ysam@cuplcs.net 48:44.744 |SIPSubs.cpp:1037:
from=<sip:fbear@cuplcs.net> to=<sip:ysam@cuplcs.net>
local_contact=sip:10.53.56.17:5080;transport=TCP
remote_contact=sip:ysam@cuplcs.net
```

XCP Router のログの例

```
12:29:24.762 |debug sdns_plugin-1.gwydlvm453 sdns_plugin handling:<presence
 type='subscribed' to='ysam@cuplcs.net'
from='bbird@cuplcs.net'><status>Already Subscribed</status></presence>
12:29:24.762 |debug ConnectionPool.cpp:166 connection pool checkout:
ccm2/dbuser (success) 12:29:24.762 |debug IdsODBC.cpp:648 Performing SQL
 operation select userid, jsmid from enduser, enterprisenode where
my_lower(xep106userid) = my_lower(?) and primarynodeid=id 12:29:24.763
|debug ODBCConnection.cpp:315 (elapsed 0.002407) select userid, jsmid
from enduser, enterprisenode where my_lower(xep106userid) = my_lower(?)
and primarynodeid=id 12:29:24.763 |debug CUPDatabaseAlgorithm.cpp:311
This is probably a Partitioned OCS user ... redirecting to
cm-3-sip-fed-s2s.gwydlvm453 component 12:29:24.763 |debug IdsODBC.cpp:229
 (elapsed 0.000137) rollback 12:29:24.763 |debug ConnectionPool.cpp:207
connection pool checkin: ccm2/dbuser (success) 12:29:24.763 |debug
```

```
sdns_plugin-1.gwydlvm453 sdns_plugin redirecting to:
cm-3-sip-fed-s2s.gwydlvm453
```

[Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] GUI 上では、SIP Proxy、XCP SIP Federation Connection Manager、および XCP Router のデバッグ トレースを有効にできます。

IM and Presence でのトレースの設定

次の手順では、[Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] GUI 上で、SIP Proxy、XCP SIP Federation Connection Manager、および XCP Router のデバッグ トレースを設定する方法について説明します。 トレース用に設定するサービスごとに、この手順を繰り返します。

注意 デバッグ レベル トレースは、システム パフォーマンスに影響を与えることがあります。 必要なときにのみデバッグ トレース レベルを有効にし、システム調査が完了した後、ログの設定をデフォルトにリセットします。

手順

ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [追跡（Trace）] > [設定（Configuration）] を選択します。

ステップ 2 IM and Presence サーバを選択し、[移動（Go）] を選択します。

ステップ 3 [サービス グループ（Service Group）] ドロップダウン リストから [IM and Presence サービス（IM and Presence Services）] を選択し、[移動（Go）] を選択します。

ステップ 4 [サービス（Service）] ドロップダウン リストから次のオプションのいずれかを選択し、[移動（Go）] を選択します。

a) SIP Proxy
b) XCP SIP Federation Connection Manager
c) XCP Router

ステップ 5 [トレース開始（Trace On）] を選択します。

ステップ 6 [トレース フィルタ設定（Trace Filter Settings）] の中で、[デバッグ トレース レベル（Debug Trace Level）] を選択します。 トレースに対してデバッグ レベル トレースを有効にしたい場合は、[デバッグ（Debug）] を選択します。

ステップ 7 SIP Proxy 向けにトレースを有効にする場合、[トレース フィルタ設定（Trace Filter Settings）] にさまざまなトレース オプションがあります。 次のトレースを選択します。

a) SIP TCP のトレースのイネーブル化（Enable SIP TCP Trace）
b) SIP TLS のトレースのイネーブル化（Enable SIP TLS Trace）
c) Server のトレースのイネーブル化（Enable Server Trace）
d) SIP メッセージとステート マシンのトレースのイネーブル化（Enable SIP Message and State Machine Trace）

e) Method/Event ルーティングのトレースのイネーブル化（Enable Method/Event Routing Trace）
f) Routing のトレースのイネーブル化（Enable Routing Trace）

ステップ 8 [保存（Save）] を選択します。
これらのサービスごとにデバッグ トレースを開始するための詳細については、Cisco Unified IM and Presence のサービスアビリティ オンライン ヘルプを参照してください。

関連トピック

LCS/OCS SIP のトレース, （110 ページ）

LCS/OCS SIP のトレース

LCS/OCS SIP Proxy コンポーネントは、すべての SIP 要求のルーティングを担当します。 ルーティングに関する問題をデバッグするには、LCS/OCS サーバ（Standard Edition または Enterprise Edition）でデバッグ トレースを有効にできます。 デバッグ トレースを開始する手順は、LCS と OCS との間で異なります。

LCS 上での SIP トレースの有効化

次の手順は、LCS 上で SIP トレースを有効にする方法について説明します。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Live Communications Server 2005] を選択します。

ステップ 2 LCS サーバの FQDN を右クリックし、[プロパティ（Properties）] を選択します。

ステップ 3 [ロギング（Logging）] タブを選択し、[ロギングを有効にする（Enable Logging）] チェックボックスをオンにします。

ステップ 4 [ロギング レベル（Logging Level）] を **4**（デバッグ）に設定します。

ステップ 5 ログ ファイルを保存する場所を選択します。

ステップ 6 その他のすべてのデフォルトを受け入れ、[OK] を選択し、[プロパティ（Properties）] ウィンドウを閉じてロギングを有効にします。

ステップ 7 ロギングを停止する準備が整った場合は、LCS サーバの FQDN を選択し、再度 [プロパティ（Properties）] を選択します。

ステップ 8 [ロギング（Logging）] タブを選択し、[ロールオーバーをすぐに強制する（Force Rollover Now）] を選択します。

ステップ 9 [ロギングを有効にする（Enable Logging）] チェックボックスをオフにして [OK] を選択し、[プロパティ（Properties）] ウィンドウを閉じます。

ステップ 10 選択した場所に最新のログ ファイルを開きます。

ステップ 11 ログのより構造化された分析を行うには、Snooper ツールをダウンロードし、それを使ってログ ファイルを表示します。

OCS 上での SIP トレースの有効化

次の手順は、OCS 上で SIP トレースを有効にする方法について説明します。

手順

ステップ 1 [スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [Office Communications Server 2007 R2] を選択します。

ステップ 2 エディションに応じて、次のいずれかを実行します。

a) Standard Edition をご使用の場合は、OCS サーバ名を右クリックし、[ログ ツール（Logging Tool）] > [新しいデバッグ セッション（New Debug Session）] を選択します。

b) Enterprise Edition をご使用の場合は、OCS プール名を右クリックし、[ログ ツール（Logging Tool）] > [新しいデバッグ セッション（New Debug Session）] を選択します。

ステップ 3 [コンポーネント（Components）] 領域で [SIPStack] チェックボックスをオンにし、[レベル（Level）] 領域で [すべて（All）] を選択します。

ステップ 4 ロギングを開始する準備が整ったら、[ログの開始（Start Logging）] を選択します。

ステップ 5 ロギングを停止する準備が整ったら、[ログの停止（Stop Logging）] を選択します。

ステップ 6 OCS SIP Proxy ログ分析を表示するには、[ログ ファイルの解析（Analyze Log Files）] を選択します。

関連トピック

IM and Presence のトレース, （107 ページ）
Snooper ツール

統合の一般的な問題

次のリストは、統合の一般的な問題のリストです。

IM and Presence ユーザが連絡先リストにユーザを追加すると、Microsoft Office Communicator ユーザがポップアップを受信しない

トラブルシューティングの手順

1. 連絡先に関して、有効な利用可能状態が表示されている場合は、Microsoft Office Communicator ユーザが IM and Presence クライアント ユーザから以前にサブスクリプションを受け入れたかどうか確認します。

   LCS/OCS サブスクリプションの許可は永続的です。つまり、IM and Presence クライアント ユーザがMicrosoft Office Communicator ユーザを削除して再度追加した場合、2 回目のポップアップは表示されません。

2. 連絡先に「確認の待機中（Waiting for Confirmation）」状態が表示される場合は、必要に応じて残りのトラブルシューティング手順を実行します。
3. 連絡先の MOC SIP URI が有効なことを確認します。
4. Cisco SIP Proxy および Cisco SIP Federation Connection Manager サービスが各 IM and Presence サーバで実行中であることを確認します。
5. パーティション化されたイントラドメイン フェデレーションが IM and Presence クラスタごとに有効であることを確認します。
6. パーティション化されたフェデレーションのルーティング モードが選択した配置に適用されるか確認します。

   拡張ルーティングは、シングル クラスタの IM and Presence 配置でのみサポートされています。

7. IM and Presence のスタティック ルートが LCS/OCS に要求をルーティングするように正しく設定されているか確認します。 これを行うには、IM and Presence ユーザのホーム ノードにある SIP Proxy ログを確認し、SIP Proxy が LCS/OCS に対する SIP NOTIFY 要求の SIP 408 要求タイムアウト エラーを返すかどうか確認します。
8. TLS 暗号化が設定されている場合、Wireshark または同等の監視ツールを使用して、TLS ハンドシェイクが成功したことを確認します。
9. TLS 暗号化が設定されているけれども、TLS ハンドシェイクが失敗する場合は、FIPS が LCS/OCS サーバで有効になっているか確認します。
10. それでも TLS ハンドシェイクが失敗する場合、さらなる TLS トラブルシューティング手順について IM and Presence と LCS/OCS との間の TLS ハンドシェイク エラー, （119 ページ） をご覧ください。
11. SIP NOTIFY を送信している IM and Presence サーバ向けに LCS/OCS ホスト認証のエントリが存在することを確認します。
12. 少なくとも IM and Presence サーバごとに IP アドレス エントリが存在する必要があります。
13. TLS 暗号化を設定すると、IM and Presence サーバ向けに 2 つ目の FQDN エントリも必要になります。

IM and Presence ユーザが連絡先リストにユーザを追加したけれども、Microsoft Office Communicator ユーザの承認時に表示されない場合、Microsoft Office Communicator ユーザがポップアップを受信する

トラブルシューティングのヒント

IM and Presence のアクセス コントロール リスト（ACL）がすべての LCS/OCS サーバ/プールからの要求を許可することを確認します。 ACL の問題がある場合、IM and Presence サーバのルーティングの SIP Proxy ログの中に「ACL - upstream not trusted - need to authenticate」というエントリが表示されます。

Microsoft Office Communicator ユーザが連絡先リストにユーザを追加しても IM and Presence ユーザがポップアップを受信しない

トラブルシューティングの手順

1. 有効な利用可能状態が表示されている場合は、ローカルのプレゼンス ドメイン内のユーザからのサブスクリプション要求を自動的に承認するように IM and Presence が設定されているか確認します。 この機能が有効な場合、IM and Presence は IM and Presence ユーザにポップアップを表示することなく、自動的に要求を承認します。
2. そうでない場合、「ステータスが不明（Status Unknown）」または「プレゼンスが不明（Presence Unknown）」と表示される場合は、必要に応じて残りのトラブルシューティング手順を実行します。
3. Cisco SIP Proxy および Cisco SIP Federation Connection Manager サービスが各 IM and Presence サーバで実行中であることを確認します。
4. パーティション化されたイントラドメイン フェデレーションが IM and Presence クラスタごとに有効であることを確認します。
5. パーティション化されたフェデレーションのルーティング モードが選択した配置に適用されるか確認します。

   拡張ルーティングは、シングル クラスタの IM and Presence 配置でのみサポートされています。
6. TLS 暗号化が設定されている場合、Wireshark または同等の監視ツールを使用して、TLS ハンドシェイクが成功したことを確認します。
7. TLS 暗号化が設定されているけれども、TLS ハンドシェイクが失敗する場合は、FIPS が LCS/OCS サーバで有効になっているか確認します。
8. それでも TLS ハンドシェイクが失敗する場合、さらなる TLS トラブルシューティング手順について IM and Presence と LCS/OCS との間の TLS ハンドシェイク エラー, （119 ページ） をご覧ください。

9 ルーティング IM and Presence サーバをポイントするスタティック ルートが LCS/OCS Standard Edition サーバまたは Enterprise Edition プールごとに設定されていることを確認します。

10 各 IM and Presence サーバが LCS/OCS の配置からドメイン ネーム サービス（DNS）から解決可能であることを確認します。

11 SIP NOTIFY メッセージを送信している IM and Presence サーバ向けに LCS/OCS ホスト認証のエントリが存在することを確認します。

a 少なくとも IM and Presence サーバごとに IP アドレス エントリが存在する必要があります。
b TLS 暗号化を設定すると、IM and Presence サーバ向けに 2 つ目の FQDN エントリも必要になります。

12 IM and Presence のアクセス コントロール リスト（ACL）がすべての LCS/OCS サーバ/プールからの要求を許可することを確認します。 ACL の問題がある場合、IM and Presence サーバのルーティングの SIP Proxy ログの中に「ACL - upstream not trusted - need to authenticate」というエントリが表示されます。

13 これがマルチクラスタ IM and Presence の配置である場合は、クラスタ間ピアリングが正しく設定されていることを確認します。

a 指定されたルーティング IM and Presence ノードを含むクラスタのパブリッシャ ノード上で [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。
b クラスタ間ピアのリストに IM and Presence ユーザがプロビジョニングされているクラスタ向けのピアが含まれていること、およびそのユーザの関連付けられたユーザの数が 0 より大きいことを確認します。
c クラスタ間ピアのステータスを検証するために、クラスタ間ピアを選択します。
d 強調表示されたエラーが存在しないことを確認してください。

IM and Presence ユーザから送信された IM を Microsoft Office Communicator ユーザが受信しない

トラブルシューティングの手順

1 Cisco SIP Proxy および Cisco SIP Federation Connection Manager サービスが各 IM and Presence サーバで実行中であることを確認します。

2 パーティション化されたイントラドメイン フェデレーションが IM and Presence クラスタごとに有効であることを確認します。

3 パーティション化されたフェデレーションのルーティング モードが選択した配置に適用されるか確認します。

拡張ルーティングは、シングル クラスタの IM and Presence 配置でのみサポートされています。

4 IM and Presence のスタティック ルートが LCS/OCS に要求をルーティングするように正しく設定されているか確認します。 これを行うには、IM and Presence ユーザのホーム ノードにある

SIP Proxy ログを確認し、SIP Proxy が LCS/OCS に対する SIP INVITE 要求の SIP 408 要求タイムアウト エラーを返すかどうか確認します。

5 TLS 暗号化が設定されている場合、Wireshark または同等の監視ツールを使用して、TLS ハンドシェイクが成功したことを確認します。

6 TLS暗号化が設定されているけれども、TLSハンドシェイクが失敗する場合は、FIPSがLCS/OCSサーバで有効になっているか確認します。

7 それでも TLS ハンドシェイクが失敗する場合、さらなる TLS トラブルシューティング手順について IM and Presence と LCS/OCS との間の TLS ハンドシェイク エラー, （119 ページ） をご覧ください。

8 SIP INVITE 要求を送信している IM and Presence サーバ向けに LCS/OCS ホスト認証のエントリが存在することを確認します。

a 少なくとも IM and Presence サーバごとに IP アドレス エントリが存在する必要があります。

b TLS 暗号化を設定すると、IM and Presence サーバ向けに 2 つ目の FQDN エントリも必要になります。

Microsoft Office Communicator ユーザによって送信された IM を IM and Presence ユーザが受信しない

トラブルシューティングの手順

1 Cisco SIP Proxy および Cisco SIP Federation Connection Manager サービスが各 IM and Presence サーバで実行中であることを確認します。

2 パーティション化されたイントラドメイン フェデレーションが IM and Presence クラスタごとに有効であることを確認します。

3 パーティション化されたフェデレーションのルーティング モードが選択した配置に適用されるか確認します。

拡張ルーティングは、シングル クラスタの IM and Presence 配置でのみサポートされています。

4 TLS 暗号化が設定されている場合、Wireshark または同等の監視ツールを使用して、TLS ハンドシェイクが成功したことを確認します。

5 TLS暗号化が設定されているけれども、TLSハンドシェイクが失敗する場合は、FIPSがLCS/OCSサーバで有効になっているか確認します。

6 それでも TLS ハンドシェイクが失敗する場合、さらなる TLS トラブルシューティング手順について IM and Presence と LCS/OCS との間の TLS ハンドシェイク エラー, （119 ページ） をご覧ください。

7 ルーティング IM and Presence サーバをポイントするスタティック ルートが LCS/OCS Standard Edition サーバまたは Enterprise Edition プールごとに設定されていることを確認します。

8 各 IM and Presence サーバが LCS/OCS の配置から DNS から解決可能であることを確認します。

9 SIP INVITE を送信している IM and Presence サーバ向けに LCS/OCS ホスト認証のエントリが存在することを確認します。

a 少なくとも IM and Presence サーバごとに IP アドレス エントリが存在する必要があります。
b TLS 暗号化を設定すると、IM and Presence サーバ向けに 2 つ目の FQDN エントリも必要になります。

10 IM and Presence のアクセス コントロール リスト（ACL）がすべての LCS/OCS サーバ/プールからの要求を許可することを確認します。 ACL の問題がある場合、IM and Presence サーバのルーティングの SIP Proxy ログの中に「ACL - upstream not trusted - need to authenticate」というエントリが表示されます。

11 これがマルチクラスタ IM and Presence の配置である場合は、クラスタ間ピアリングが正しく設定されていることを確認します。

a 指定されたルーティング IM and Presence ノードを含むクラスタのパブリッシャ ノード上で [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。
b クラスタ間ピアのリストに IM and Presence ユーザがプロビジョニングされているクラスタ向けのピアが含まれていること、およびそのユーザの関連付けられたユーザの数が 0 より大きいことを確認します。
c クラスタ間ピアのステータスを検証するために、クラスタ間ピアを選択します。
d 強調表示されたエラーが存在しないことを確認してください。

Microsoft Office Communicator ユーザのアップデートおよび IM の表示に最大 40 秒かかる

トラブルシューティングの手順

このような遅延の最も一般的な理由は、配置内の DNS の設定が不足していることです。 IM and Presence は、着信 SIP 要求の送り側となる LCS/OCS の IP アドレスの DNS 逆検索を実行します。 IP アドレスがホスト名に解決されない場合、逆検索は約 20 秒後にタイムアウトします。 これが発生すると、SIP Proxy ログに「incoming ACL check took over 2 seconds – check DNS」というログが表示されます。

この問題を解決するには、DNS ポインタ（PTR）レコードが LCS/OCS サーバの IP アドレスごとに存在することを確認してください。

拡張ルーティングが有効な場合、IM and Presence と LCS/OCS との間でプレゼンスが交換されない

トラブルシューティングの手順

1. Cisco Unified Communications Manager がすべての LCS/OCS ユーザ向けに Active Directory からユーザ データを同期していることを確認します。

   拡張ルーティングは、Active Directory からCisco Unified Communications Manager に同期されている LCS/OCS SIP URI に依存します。

2. これがシングルクラスタのIM and Presence配置の場合のみ、拡張ルーティングが有効であることを確認します。

IM and Presence ユーザが Microsoft Office Communicator のアドレス帳に表示されない

トラブルシューティングの手順

1. IM and Presence ユーザが OCS から移行されて以来、LCS/OCS アドレス帳サービスによる完全同期が実施されていることを確認します。 この同期は、デフォルトで毎夜実施されます。
2. Microsoft Office Communicator ユーザに、新しいアドレス帳のダウンロードをトリガするために、サインアウトしてサインインするように要求します。 デフォルトでは、Microsoft Office Communicator が LCS/OCS から新しいアドレス帳をダウンロードするのに 1 時間を超える可能性があります。
3. IM and Presence ユーザが以前は Microsoft Office Communicator ユーザだった場合は、IM and Presence ユーザの古い LCS/OCS SIP URI が Active Directory アクティブ ディレクトリに入力されていることを確認します（msRTCSIP-PrimaryUserAddress）。
4. IM and Presence ユーザが前は Microsoft Office Communicator ユーザでなかった場合、または古い LCS/OCS SIP URI が Active Directory から消去されている場合は、Active Directory の [msRTCSIP-PrimaryUserAddress] フィールドに手動で入力し、IM and Presence ユーザが Microsoft Office Communicator のアドレス帳に表示されることを確認します。 [msRTCSIP-PrimaryUserAddress] フィールドにsip:<user's uri> と入力する必要があります。

IM and Presence がドメイン間フェデレーション要求を LCS/OCS の配置経由でルーティングできない

トラブルシューティングの手順

1. LCS/OCS の配置がドメイン間フェデレーション用に正しく設定されていることを確認します。これを行うには、Microsoft Office Communicator ユーザがフェデレーションできることを確認します。
2. Cisco SIP Proxy および Cisco SIP Federation Connection Manager が各 IM and Presence サーバで実行中であることを確認します。
3. IM and Presence が外部ドメイン用にドメイン間フェデレーション用に設定されており、そのダイレクト フェデレーションが有効になっていることを確認します。
4. 外部ドメイン用にスタティック ルートが IM and Presence に設定され、スタティック ルートが LCS/OCS をポイントしていることを確認します。
5. 外部ドメインが IM and Presence のアクセス コントロール リスト（ACL）に含まれていることを確認します。

IM and Presence と LCS/OCS との間の TLS ハンドシェイク エラー

トラブルシューティングの手順

1. FIPS が各 LCS/OCS サーバ上で有効になっていることを確認します。
2. LCS/OCS がポート 5061 でお互いの TLS 接続をリッスンするように設定されていることを確認します。
3. プレゼンスのピア認証ポートが 5061 に設定されているように IM and Presence のアプリケーション リスナーが設定されていることを確認します。
4. IM and Presence 証明書が LCS/OCS サーバと同じ認証局によって署名されていることを確認します。
5. LCS/OCS または IM and Presence の証明書のいずれも有効期限切れでないことを確認します。
6. LCS/OCS 証明書がサーバ認証とクライアント認証の両方に対して設定されていることを確認します。
   - そのような証明書には、“1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2” という OID 値が含まれています。
   - 証明書がサーバ認証用にのみ設定されている場合、“1.3.6.1.5.5.7.3.1” という OID 値が含まれています。

7 IM and Presence TLS ピア サブジェクト リストに、LCS/OCS が TLS ハンドシェイク時に提供する証明書で使用される件名共通名（CN）が含まれることを確認します。

8 IM and Presence TLS ピア認証 TLS コンテキストが正しく設定されており、すべての TLS ピア サブジェクトが選択されていることを確認します。

Microsoft Office Communicator ユーザが Cisco Unified Personal Communicator の連絡先リストに追加されると、不正な SIP URI がそのユーザに指定される

トラブルシューティングの手順

Cisco Unified Personal Communicator レジストリの設定が正しいこと、特に LDAP_AttributeName_uri and LDAP_UriSchemeName サブキーが正しいことを確認します。 詳細については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』の「Configuring Active Directory for Cisco Unified Personal Communicator」の章を参照してください。

Microsoft Office Communicator の連絡先の表示名が Cisco Unified Personal Communicator に表示されない

トラブルシューティングの手順

Cisco Unified Personal Communicator レジストリの設定が正しいこと、特に LDAP_AttributeName_uri and LDAP_UriSchemeName サブキーが正しいことを確認します。 詳細については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』の「Configuring Active Directory for Cisco Unified Personal Communicator」の章を参照してください。

ユーザ移行のトラブルシューティング

ユーザ移行のトレース

連絡先リスト エクスポート ツール

連絡先リスト エクスポート ツールを使用すると、管理者はユーザの移行用に LCS/OCS から連絡先リストを一括でエクスポートすることができます。 ツールを実行するたびに、ExportContactsLog<Timestamp>.txt と呼ばれるログ ファイルが生成されます。 ログファイルには、発生した障害やエラーに関する詳細が含まれています。 ログファイルは、ツール自体と同じ場所に保存されます。

エラーが発生する一般的な原因の一部は次のとおりです。

- 不正な入力ファイル名が指定された
- 入力ファイルの中にスペルミスがある
- 指定されたユーザがツールの実行対象の LCS/OCS サーバ/プールに関連付けられていない

連絡先リスト エクスポート ツールのログ ファイルの例は次のとおりです。

```
>>------------------- 18/05/2011 16:59:38 ------------------->>Version:
2.1 [DEBUG] Enter>> ExportContacts.LdapConnection.CreateLdapDirectoryEntry
 [DEBUG] Enter>> ExportContacts.LdapConnection.CreateDirectoryEntry [DEBUG]
 Enter>> ExportContacts.LdapConnection.checkLdapPrefix [DEBUG] Exit>>
ExportContacts.LdapConnection.checkLdapPrefix [DEBUG] Exit>>
ExportContacts.LdapConnection.CreateDirectoryEntry [DEBUG] Current line
item is: sip:ExampleUser@dtstfedcup2.com [DEBUG] Exit>>
ExportContacts.ExportContactsUtilities.getAllSipUriFromStandardFile [DEBUG]
 Enter>> ExportContacts.ExportContactsUtilities.getAndPrintContactsForUsers
 [DEBUG] Total number of users found is: 1 [DEBUG] Processing user number:
 1 [INFO] Preparing to get contacts for User
[sip:ExampleUser@dtstfedcup2.com] [DEBUG] Enter>>
ExportContacts.OcsWmiConnection.getContactsAndGroupsForUser [DEBUG] Enter>>
 ExportContacts.OcsWmiConnection.getUserInstanceID [DEBUG] Searching for
 userInstanceId [SELECT * FROM MSFT_SIPESUserSetting WHERE PrimaryURI =
'sip:ExampleUser@dtstfedcup2.com'] [DEBUG] Enter>>
ExportContacts.OcsWmiConnection.GetScope [DEBUG] Exit>>
ExportContacts.OcsWmiConnection.GetScope [DEBUG] Search results returned
 [DEBUG] Found user with PrimaryURI : sip:ExampleUser@dtstfedcup2.com,
InstanceId : {7D777FD5-A8F6-8243-B4D6-7F331008C58C} [DEBUG] Exit>>
ExportContacts.OcsWmiConnection.getUserInstanceID [DEBUG] Enter>>
ExportContacts.OcsWmiConnection.getContacts [DEBUG] Searching for contacts
 [SELECT * FROM MSFT_SIPESUserContactData WHERE UserInstanceID =
'{7D777FD5-A8F6-8243-B4D6-7F331008C58C}'] [DEBUG] Enter>>
ExportContacts.OcsWmiConnection.GetScope [DEBUG] Exit>>
ExportContacts.OcsWmiConnection.GetScope [DEBUG] Search results returned
 [DEBUG] Found contact: SIPURI : [SIP:lcsContact@dtstfedcup2.com] with
GroupId: [1] [DEBUG] Found contact: SIPURI :
[SIP:ExampleUser@dtstfedcup2.com] with GroupId: [1] [DEBUG] Exit>>
ExportContacts.OcsWmiConnection.getContacts [DEBUG] Enter>>
ExportContacts.OcsWmiConnection.getGroups [DEBUG] Searching for groups
[SELECT * FROM MSFT_SIPESUserContactGroupData WHERE UserInstanceID =
'{7D777FD5-A8F6-8243-B4D6-7F331008C58C}'] [DEBUG] Enter>>
ExportContacts.OcsWmiConnection.GetScope [DEBUG] Exit>>
ExportContacts.OcsWmiConnection.GetScope [DEBUG] Search results returned
 [DEBUG] Found group: groupName : [General] with GroupId: [1] [DEBUG]
Exit>> ExportContacts.OcsWmiConnection.getGroups [INFO] User Processed
```

```
Successfully [DEBUG] Exit>>
ExportContacts.OcsWmiConnection.getContactsAndGroupsForUser [DEBUG] Enter>>
 ExportContacts.ExportContactsUtilities.PrintContactsForUser [DEBUG]
Exit>> ExportContacts.ExportContactsUtilities.PrintContactsForUser [DEBUG]
 Exit>> ExportContacts.ExportContactsUtilities.getAndPrintContactsForUsers
 [INFO] Summary: [INFO] 1 users successfully processed [INFO] 0 users not
 found [INFO] 0 users could not be processed due to errors
<<------------------- 18/05/2011 16:59:41 -------------------<<
```

関連トピック

IM and Presence BAT による連絡先リストのインポート, （124 ページ）

アカウント無効化ツール

アカウント無効化ツールは、Active Directory（AD）に接続し、ユーザの LCS/OCS 属性を更新して LCS/OCS アカウントを無効にします。 ツールを実行するたびに、DisableAccountLog<Timestamp>.txt と呼ばれるログ ファイルが生成されます。 ログファイルには、発生した障害やエラーに関する詳細が含まれています。 ログファイルは、ツール自体と同じ場所に保存されます。

このツールでエラーが発生する一般的な原因の一部は次のとおりです。

- 不正な入力ファイル名が指定された
- 入力ファイルの中にスペルミスがある
- ユーザが LCS/OCS データベースに存在しない
- ツールを実行している管理者が AD に対する読み取り/書き込み権限を持っていない
- このツールによって AD に変更内容が適用され、LCS/OCS データベースまで伝播するのに必要な時間を管理者が十分に設けていない。 変更が LCS/OCS データベースに反映されていることを検証せずに、管理者が次の移行ステップに進んだ場合、移行が失敗することがある。

アカウント無効化ツールのログ ファイルの例は次のとおりです。

```
>>------------------- 18/05/2011 17:02:07 -------------------->>Version:
2.0 [DEBUG] Enter>> DisableAccount.LdapConnection.CreateLdapDirectoryEntry
 [DEBUG] Enter>> DisableAccount.LdapConnection.CreateDirectoryEntry [DEBUG]
 Enter>> DisableAccount.LdapConnection.checkLdapPrefix [DEBUG] Exit>>
DisableAccount.LdapConnection.checkLdapPrefix [DEBUG] Exit>>
DisableAccount.LdapConnection.CreateDirectoryEntry [DEBUG] Enter>>
DisableAccount.AccountDisable.DisableUsersInFile [DEBUG] Enter>>
DisableAccount.AccountDisable.GetSipUriFromLine [DEBUG] Exit>>
DisableAccount.AccountDisable.GetSipUriFromLine [INFO] Preparing to Disable
 Communications Server Account for User [sip:ExampleUser@dtstfedcup2.com]
 [DEBUG] Enter>> DisableAccount.LdapConnection.DisableAccount [INFO]
Searching for user [sip:ExampleUser@dtstfedcup2.com] [INFO] Search results
 returned [DEBUG] Enter>>
DisableAccount.LdapConnection.CreateLdapDirectoryEntry [DEBUG] Enter>>
DisableAccount.LdapConnection.CreateDirectoryEntry [DEBUG] Enter>>
DisableAccount.LdapConnection.checkLdapPrefix [DEBUG] Exit>>
DisableAccount.LdapConnection.checkLdapPrefix [DEBUG] Exit>>
DisableAccount.LdapConnection.CreateDirectoryEntry [INFO] Found user with
```

```
 PrimaryURI : sip:ExampleUser@dtstfedcup2.com, DisplayName : Example User,
 Enabled : True [DEBUG] Committed changes to the AD [INFO] User Account
Disabled [DEBUG] Exit>> DisableAccount.LdapConnection.DisableAccount
[DEBUG] Enter>> DisableAccount.AccountDisable.GetSipUriFromLine [DEBUG]
Exit>> DisableAccount.AccountDisable.DisableUsersInFile [INFO] Summary:
[INFO] 1 users successfully processed [INFO] 0 users not found [INFO] 0
users could not be processed due to errors <<------------------- 18/05/2011
 17:02:08 --------------------<<
```

関連トピック

アカウント削除ツール, （123 ページ）

アカウント削除ツール

アカウント削除ツールを使用すると、移行するユーザを削除することで、それらのユーザへのプレゼンス要求が後から IM and Presence にルーティングされるようにします。その一方で、削除されたユーザは、LCS/OCS に残っているユーザの連絡先リストからは削除されません。アカウント削除ツールを実行すると、DeleteAccountLog<Timestamp>.txt と呼ばれるログ ファイルがツールと同じディレクトリに生成されます。 ログファイルには、発生した障害やエラーに関する詳細が含まれています。

このツールでエラーが発生する一般的な原因の一部は次のとおりです。

- 不正な入力ファイル名が指定された
- 不正なデータベース インスタンス名が指定された
- 入力ファイルの中にスペルミスがある
- ユーザが LCS/OCS データベースに存在しない

アカウント削除ツールのログ ファイルの例は次のとおりです。

```
>>------------------- 18/05/2011 17:03:26 ------------------->>Version:
2.0 [DEBUG] Enter>> DeleteAccount.DbConnectionFactory.GetCommSvrDbCon
[DEBUG] Enter>> DeleteAccount.DbConnectionFactory.GetConnection [DEBUG]
Attempting to Open connection with String :
Server=10.53.46.132\lcsdatabase;Database=rtc;Trusted_Connection=yes;
[DEBUG] Connection Opened Ok [DEBUG] Exit>>
DeleteAccount.DbConnectionFactory.GetConnection [DEBUG] Enter>>
DeleteAccount.DbConnectionFactory.tableExists [DEBUG] SQL is [SELECT id
FROM sysobjects WHERE name = 'Resource'] [DEBUG] Found id [517576882]
[DEBUG] Exit>> DeleteAccount.DbConnectionFactory.tableExists [INFO] Found
 the Resource Table, appears to be a valid Communications Server Database
 [DEBUG] Enter>> DeleteAccount.DbConnectionFactory.tableExists [DEBUG]
SQL is [SELECT id FROM sysobjects WHERE name = 'Endpoint'] [DEBUG] Found
 id [2098106515] [DEBUG] Exit>>
DeleteAccount.DbConnectionFactory.tableExists [INFO] Found the Endpoint
table, Creating LCS Database Connection [DEBUG] Exit>>
DeleteAccount.DbConnectionFactory.GetCommSvrDbCon [DEBUG] Enter>>
DeleteAccount.CommSvrDbConnection.CheckConnection [DEBUG] Enter>>
DeleteAccount.CommSvrDbConnection.GetConnection [DEBUG] Exit>>
DeleteAccount.CommSvrDbConnection.GetConnection [DEBUG] Exit>>
DeleteAccount.CommSvrDbConnection.CheckConnection [DEBUG] Enter>>
```

```
DeleteAccount.DeleteUserData.DisableUsersInFile [DEBUG] Enter>>
DeleteAccount.DeleteUserData.GetUserAtHostFromLine [DEBUG] Exit>>
DeleteAccount.DeleteUserData.GetUserAtHostFromLine [INFO] Preparing to
Delete Communications Server Data for User [ExampleUser@dtstfedcup2.com]
 [DEBUG] Enter>> DeleteAccount.DeleteUserData.DeleteOcsUserData [DEBUG]
Enter>> DeleteAccount.CommSvrDbConnection.GetResourceIdForUser [DEBUG]
Enter>> DeleteAccount.CommSvrDbConnection.GetConnection [DEBUG] Exit>>
DeleteAccount.CommSvrDbConnection.GetConnection [DEBUG] Enter>>
DeleteAccount.CommSvrDbConnection.SqlEscape [DEBUG] Exit>>
DeleteAccount.CommSvrDbConnection.SqlEscape [DEBUG] Exit>>
DeleteAccount.CommSvrDbConnection.GetResourceIdForUser [INFO] Found user
 [ExampleUser@dtstfedcup2.com] with ResourceId [402], proceeding to delete
 data [DEBUG] Enter>> DeleteAccount.LcsDbConnection.DeleteResourceDirectory
 [DEBUG] Enter>> DeleteAccount.CommSvrDbConnection.GetConnection [DEBUG]
 Exit>> DeleteAccount.CommSvrDbConnection.GetConnection [DEBUG] Deleted
SubscriptionStatic for resource [402] [DEBUG] Deleted SubscriptionDynamic
 for resource [402] [DEBUG] Deleted BatchSubChild for resource [402]
[DEBUG] Deleted HomedResourceRegisterTime for resource [402] [DEBUG]
Deleted HomedResourcePermission for resource [402] [DEBUG] Deleted
BatchSubParent for resource [402] [DEBUG] Deleted Endpoint for resource
[402] [DEBUG] Deleted ContactGroupAssoc for resource [402] [DEBUG] Deleted
 ContactGroup for resource [402] [DEBUG] Deleted Contact for resource
[402] [DEBUG] Deleted HomedResource for resource [402] [DEBUG] Deleted
ResourceDirectory for resource [402] [DEBUG] Committing transaction for
resource [402] [INFO] Completed Updates for resource [402] [DEBUG] Exit>>
 DeleteAccount.LcsDbConnection.DeleteResourceDirectory [DEBUG] Exit>>
DeleteAccount.DeleteUserData.DeleteOcsUserData [DEBUG] Enter>>
DeleteAccount.DeleteUserData.GetUserAtHostFromLine [DEBUG] Exit>>
DeleteAccount.DeleteUserData.GetUserAtHostFromLine [DEBUG] Exit>>
DeleteAccount.DeleteUserData.DisableUsersInFile [INFO] Summary: [INFO] 1
 users successfully processed [INFO] 0 users not found [INFO] 0 users
could not be processed due to errors <<-------------------- 18/05/2011
17:03:27 --------------------<<
```

関連トピック

アカウント無効化ツール，（29 ページ）

IM and Presence BAT による連絡先リストのインポート

IM and Presence 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。
- 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。

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。

2 [検索（Find）] を選択し、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。

3 [ログ ファイル名（Log File Name）] リンクを選択し、ログを開きます。

任意の BAT ジョブの詳細が必要な場合は、一括プロビジョニング サービスのデバッグ ログを参照してください。 これらのログには、/var/log/active/cm/trace/bps/log4j/bps000*.txt からアクセスできます。

一括プロビジョニング サービスのデバッグ ロギングは、[Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] GUI から有効にできます。

IM and Presence での BAT プロビジョニング サービスでのロギングの設定

次の手順では、IM and Presence で BAT プロビジョニング サービスでロギングを設定する方法について説明します。

注意 デバッグ レベル トレースは、システム パフォーマンスに影響を与えることがあります。 必要なときにのみデバッグ トレース レベルを有効にし、システム調査が完了した後、ログの設定をデフォルトにリセットします。

手順

ステップ 1 [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] > [トレース（Trace）] > [設定（Configuration）] を選択します。

ステップ 2 IM and Presence サーバを選択し、[移動（Go）] を選択します。

ステップ 3 [サービス グループ（Service Group）] ドロップダウン リストから [データベースおよび管理者サービス（Database and Admin Services）] を選択し、[移動（Go）] を選択します。

ステップ 4 [サービス（Service）] ドロップダウン リストから [一括プロビジョニングサービス（Bulk Provisioning Service）] を選択し、[移動（Go）] を選択します。

ステップ 5 [トレース開始（Trace On）] を選択します。

ステップ 6 [トレース フィルタ設定（Trace Filter Settings）] の中で、[デバッグ トレース レベル（Debug Trace Level）] を選択します。 トレースに対してデバッグ レベルを有効にしたい場合は、[デバッグ（Debug）] を選択します。

ステップ 7 [保存（Save）] を選択します。

関連トピック

連絡先リスト エクスポート ツール, （121 ページ）

ユーザ移行の一般的な問題

アプリケーションが正しく初期化できない - ユーザ移行ツールのいずれかを実行しているときにエラーが発生する

トラブルシューティングの手順

シスコが提供する各ユーザ移行ツールを使用するには、.NET Framework の少なくともバージョン 1.1 が、そのツールを実行している場所からサーバにインストールされている必要があります。.NET 1.1 以降が自分のコンピュータにインストールされていることを確認します。

連絡先リスト エクスポート ツール - ログの概要にいくつかのユーザが見つからないと表示される

トラブルシューティングの手順

1. IM and Presence のエクスポート済みファイルを入力として使用する場合は、正しいドメインが -d/ パラメータに使用され、ファイル内に入力ミスがないことを確認してください。
2. SIP URI ファイルを入力ファイルとして使用している場合は、ユーザが有効（Active Directory [AD] および LCS/OCS に存在する）で、入力ファイルに「sip:」プレフィックス付きで正しく入力されていることを確認します。
3. IM and Presence のエクスポートされたファイルあるいは SIP URI ファイルを入力に使用している場合、または OU 入力ファイルを使用している場合、ユーザ アカウントが AD の中で無効になっている可能性が高いです。 ユーザ アカウントを再度有効にし、このツールを再度実行してください。

連絡先リスト エクスポート ツール - 通常モードで実行すると、ツールは経過表示バーを表示せず、エクスポートされた連絡先の出力ファイルを生成しない

トラブルシューティングの手順

1. 連絡先リスト エクスポートのログに次のエラーがないか確認します。「次の IP/FQDN/ホスト名を使用して LDAP に接続することができません：[some_ip_or_hostname]（Unable to connect to LDAP using IP/FQDN/Hostname: [some_ip_or_hostname]）」
   a. エラーが存在する場合は、Active Directory（AD）サーバ用に指定されたアドレスが正しいか確認します。
   b. 指定したアドレスが有効な場合は、AD サーバと LCS/OCS サーバ間のネットワークが接続されていることを確認するために AD サーバに ping を実行します。
   c. 接続が確立されている場合、ADサーバにアクセスするのに必要な権限をユーザが持っていることを確認します。
2. 連絡先リストエクスポートのログに次のエラーがないか確認します。「ファイルを開くことに失敗しました…（Failed to open file…）」
   1. エラーが存在する場合は、-f/ パラメータに使用されるファイル名のスペルが間違っているか無効です。
   2. 入力ファイルのファイル名にスペースや特殊文字が含まれていないことも確認してください。

アカウント無効化ツール - ログには、IP/FQDN/ホスト名を使用して LDAP に接続できないことが記載されている

トラブルシューティングの手順

1. Active Directory（AD）サーバ用に指定されたアドレスが正しいか確認します。
2. 指定したアドレスが有効な場合は、AD サーバと LCS/OCS サーバ間のネットワークが接続されていることを確認するために AD サーバに ping を実行します。
3. 接続が確立されている場合、AD サーバにアクセスするのに必要な権限をユーザが持っていることを確認します。

アカウント削除ツール - LCS/OCS データベースまたは SQL サーバ インスタンスが見つからない

トラブルシューティングの手順

1. アカウントが正しく削除されていることを確認するには、各データベースインスタンス（OCS）と SQL サーバ インスタンス（LCS）に対してアカウント削除ツールを実行する必要があります。
2. OCS の場合、次の手順に従って各サーバ/プールのデータベース インスタンスを見つけます。
   a. OCS 管理コンソールで、[Enterprise プール（Enterprise Pools）] からプール名を選択するか（Enterprise Edition）、[Standard Edition サーバ（Standard Edition Servers）] からサーバ名を選択します（Standard Edition）。
   b. 右側のペインで [データベース（Database）] タブを選択します。
   c. データベースのインスタンス名は、[全般設定（General Settings）] の最初の項目です。
3. LCS の場合、次の手順に従って各サーバ/プールの SQL サーバ インスタンスを見つけます。
   a. [フォレスト（Forest）] > [ドメイン（Domains）] > [<domain name>] > [Live Communications のサーバおよびプール（Live Communications servers and pools）] > [<pool name>] からプール名を選択します。
   b. 右側のペインで [ステータス（Status）] タブを選択します。
   c. 最初の項目は、SQL サーバ インスタンスです。

アカウント削除ツール - SQL Server への接続中にログにエラーが表示される

トラブルシューティングの手順

1. アカウント削除ツールのログをチェックし、このエラーのログを確認します。エラーが「このユーザは SQL Server の信頼関係接続と関連付けられていません。（The user is not associated with

a trusted SQL Server connection）」である場合、ツールを実行しているユーザが、LCS/OCS データベースに書き込むために必要な権限を持っていません。

2 必要な権限を持つユーザ アカウントを使用してツールを再実行してください。

BAT 連絡先リストの更新 - アップロードされた連絡先リスト ファイルがドロップダウン リストに表示されない

トラブルシューティングの手順

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、[検索（Find）] を選択します。

2 ファイルが存在し、その機能タイプが [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）] であることを確認します。

3 不正な機能タイプのファイルが存在する場合、そのファイルを削除します。 ファイルを削除したか、ファイルが存在しない場合は、もう一度ファイルをアップロードし、そのターゲットが [連絡先リスト（Contact Lists）] であり、そのトランザクション タイプが [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）] であることを確認します。

BAT 連絡先リストの更新 - BAT ジョブの後にログ ファイルが結果ページ上に存在しない

トラブルシューティングの手順

BAT の連絡先インポート ジョブのログがジョブの結果ページから欠落している場合、BAT ジョブはサブスクライバ ノードから実行されました。 ログは、パブリッシャ ノードからのみアクセス可能です。 ログを表示するには、パブリッシャ ノード上の [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] にサインインします。

BAT 連絡先リストの更新 - ユーザの連絡先が BAT ジョブ中にインポートされない

トラブルシューティングの手順

1 具体的なエラーがないかジョブ結果のログ ファイルをチェックします。

2 IM and Presence に対して、ユーザにライセンスが付与されていることを確認します。

3 ユーザがこのクラスタ内のノードに割り当てられていることを確認します。

4 連絡先のドメインが有効であることを確認します。

BAT 連絡先リストの更新 - ユーザの連絡先が BAT ジョブ中に部分的にインポートされる

トラブルシューティングの手順

1. 具体的なエラーがないかジョブ結果のログ ファイルをチェックします。
2. 欠落している連絡先が、CSV ファイル内で有効な形式で入力されていることを確認します。
3. 連絡先のユーザ数が、システムの [連絡先リストの最大サイズ（Maximum Contact List Size）] を超えていないか確認します。
4. ウォッチャのユーザ数が、システムの [ウォッチャの最大数（Maximum Watchers）] を超えていないか確認します。

BAT 連絡先リストの更新 - 連絡先が BAT ジョブ中にインポートされない

トラブルシューティングの手順

1. 具体的なエラーがないかジョブ結果のログ ファイルをチェックします。
2. インポート ファイルが、有効な形式で入力されていることを確認します。
3. IM and Presence に対して、すべてのユーザにライセンスが付与されていることを確認します。
4. すべてのユーザがローカル クラスタ上で割り当てられていることを確認します。
5. Cisco Presence Engine サービスがクラスタ内のすべてのノードで実行中であることを確認します。

移行処理中に、ユーザの移行が [ステータスが不明（Status Unknown）] または [プレゼンスが不明（Presence Unknown）] の状態で Microsoft Office Communicator ユーザに表示される

トラブルシューティングの手順

1. このドキュメントで説明したように、連絡先が IM and Presence に完全に移行されていることを確認します。

   マイグレーション プロセス中、連絡先の移行のプレゼンスを Microsoft Office Communicator ユーザが利用できない期間があります。シスコでは、そのような問題がなるべく発生しないようにするために、予定されたメンテナンス ウィンドウの中でユーザ移行を実行することをお勧めします。
2. Microsoft Office Communicator ユーザにサインアウトして再度サインインするように依頼します。

移行された連絡先が IM and Presence にインポートされたら、Microsoft Office Communicator ユーザには、Microsoft Office Communicator クライアントからサインアウトしてサインインするまでそれらの連絡先のプレゼンスが表示されません。

3 問題が解決しない場合は、このドキュメントで説明したように移行手順が正しく実行されたことを確認します。

- アカウント削除ツールを実行する前に、アカウント無効化ツールによって適用された更新が LCS/OCS に同期されたことを確認します。
- すべての LCS/OCS Standard Edition サーバまたは Enterprise Edition プールでアカウント管理ツールが実行されたことを確認します。
- これらの手順が正しく実行されなかった場合は、次の手順を繰り返してこの問題を解決します。
  - アカウント無効化ツールを実行する
  - アカウント無効化ツールによって実行された更新が LCS/OCS に同期されたことを確認する
  - アカウント削除ツールを実行する

4 それでも移行した連絡先が [プレゼンスが不明（Presence Unknown）] と表示される場合は、IM and Presence と LCS/OCS との間の統合に問題がある可能性があります。 統合の問題のトラブルシューティングに関するヘルプについては、統合の一般的な問題, （112 ページ）を参照してください。