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 サービス ノードの設定

パーティションイントラドメインフェデレーションのドメイン設定

パーティション イントラドメイン フェデレーションの IM and Presence サービスをセット アップする前に、IM and Presence サービス クラスタのすべてのノードで必要なプレゼンス ドメインがすべて設定されていることを確認します。Skype for Business/Lync/OCS サーバに一致するプレゼンス ドメインがあること確認します。必要に応じて、**Cisco Unified IM and Presence Administration** ユーザ インターフェイスを使用して、クラスタ内のノードでローカル プレゼンス ドメインを追加するか更新します。

ディレクトリ URI が IM アドレス スキームとして設定されている場合に複数のドメインが IM and Presence サービス クラスタでサポートされます。クラスタ内のすべてのノードは IM アドレス スキームとしてディレクトリ URI を使用するディレクトリ URI をサポートする必要があります。

クラスタに対して Directory URI IM アドレス スキームを設定する詳細に関しては、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

ドメイン間フェデレーションの複数のドメインのセットアップについては『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager Guide*』を参照してください。

IM アドレス ドメインの表示

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

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

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

- ドメイン
- ローカル クラスタで使用中
- ピアのクラスタで使用中

手順

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

フェデレーションの IM and Presence 設定タスク フロー

はじめる前に

すべての必要なプレゼンス ドメインが IM and Presence サービス クラスタのすべてのノードで設定されていることを確認します。詳細は、パーティションイントラドメインフェデレーションのドメイン設定, （1 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	ルーティング ノードの設定, （4 ページ）	（オプション）複数のノードを含むチャット専用展開の場合は、専用のルーティング ノードを選択し、ルーティング ノードで不要なサービスを非アクティブにします。

	コマンドまたはアクション	目的
		（注） チャット＋通話の展開または単一ノード展開の場合は、専用のルーティング ノードは必要なく、このタスクをスキップできます。
ステップ 2	クラスタの機能サービスの開始, （5 ページ）	IM and Presence サービス クラスタ ノードで必要不可欠なサービスを開始します。
ステップ 3	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, （6 ページ）	IM and Presence サービスでパーティション イントラドメイン フェデレーションおよびルーティングのオプションを有効にします。
ステップ 4	Microsoft Lync へのスタティック ルートの設定, （7 ページ）	スタティック ルートを Lync/OCS 展開に設定します。 （注） Lync の場合は、TLS スタティック ルートを作成します。OCS の場合は、TCP または TLS ルートを作成できます。
ステップ 5	着信アクセス コントロール リストの設定, （9 ページ）	Lync/OCS サーバが認証なしで IM and Presence にアクセスできるように、着信アクセス コントロール リストを IM and Presence に設定します。
ステップ 6	アプリケーション リスナー ポートを設定します。, （11 ページ）	IM and Presence サービスで、サーバ認証とピア認証の両方のデフォルト Cisco SIP プロキシ TLS リスナー ポート値を変更します。
ステップ 7	TLS ピア サブジェクトの設定, （12 ページ）	Lync/OCS サーバと Expressway Gateway（チャット＋通話シナリオ）の TLS ピア サブジェクトを設定します。
ステップ 8	ピア認証 TLS コンテキストの設定, （14 ページ）	ピア認証を設定します。
ステップ 9	認証局のルート証明書のインポート, （15 ページ）	CA のルート証明書を IM and Presence サービスの信頼ストアにアップロードします。
ステップ 10	IM and Presence サービスの証明書署名要求の生成, （16 ページ）	CA 署名付き証明書の要求
ステップ 11	認証局からの署名付き証明書のインポート, （17 ページ）	IM and Presence サービスから CSR を生成し、ダウンロードします。
ステップ 12	Expressway Gateway の設定, （18 ページ）	（オプション）Lync によるチャット＋通話フェデレーションの場合は、Expressway Gateway を展開します。

	コマンドまたはアクション	目的
		（注） チャット専用の展開では、またはOCSを使用してフェデレーションを設定するときは、Expressway Gateway を展開する必要はありません。

ルーティング ノードの設定

マルチノード チャット専用の展開では、ルーティング ノードとして機能する IM and Presence サービス クラスタ ノードを選択します。ルーティングに余分な容量を提供するには、ルーティング ノードにユーザを割り当ててはいけません。ルーティング ノードはフロントエンドサーバとして機能し、Lync/OCS からの着信 SIP 要求を受け取り、これらの要求を受信者のホームである適切なクラスタ ノードにルーティングします。

（注） Lync を使用したチャット + 通話の展開の場合、および単一ノード展開の場合は、ルーティング ノードを設定する必要がないため、この手順をスキップできます。

手順

ステップ 1 [Cisco Unified CM IM and Presenceのサービスアビリティ（Cisco Unified IM and Presence Serviceability）] ユーザ インターフェイスから、[ツール（Tools）]>[サービスのアクティブ化（Service Activation）] を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン メニューから、ルーティング ノードとして指定するクラスタ ノードを選択します。ルーティング ノードにはユーザを割り当ててはいけません。

ステップ 3 [Cisco SIP Proxy] 機能サービスをオンにします。

ステップ 4 次の機能サービスをオフにします。

- 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 5 [保存（Save）] をクリックします。

ステップ 6 CIsco XCP Router ネットワーク サービスが実行中であることを確認します。サービスはネットワーク サービスであるため、以前に無効にしていない限り、デフォルトで実行されています。

a) [ツール（Tools）] > [コントロール センター - ネットワーク サービス（Control Center - Network Services）] を選択します。

b) [サーバ（Server）] ドロップダウン メニューから、ルーティング ノードを選択し、[移動（Go）] をクリックします。

c) CIsco XCP Router サービスが実行されていない場合は、対応するオプション ボタンをオンにし、[開始（Start）] をクリックします。

次の作業

クラスタの機能サービスの開始, （5 ページ）

クラスタの機能サービスの開始

IM and Presence サービス クラスタ ノードに不可欠な機能サービスを開始します。マルチノード チャット専用展開の場合は、ルーティング ノードを除くすべてのノードに対しこのタスクを完了します。それ以外の場合は、すべてのクラスタ ノードに対しこのタスクを完了します。

手順

ステップ 1 [Cisco Unified CM IM and Presenceのサービスアビリティ（Cisco Unified IM and Presence Serviceability）] インターフェイスから、[ツール（Tools）] > [サービスのアクティブ化（Service Activation）] を選択します。

ステップ 2 [サーバ（Server）] メニューから、クラスタ ノードを選択し、[移動（Go）] をクリックします。

ステップ 3 次のサービスを確認します。

- Cisco SIP Proxy
- Cisco XCP SIP Federation Connection Manager

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 CIsco XCP Router ネットワーク サービスが実行中であることを確認します。サービスはネットワーク サービスであるため、以前に無効にしていない限り、デフォルトで実行されています。

a) [ツール（Tools）] > [コントロール センター - ネットワーク サービス（Control Center - Network Services）] を選択します。

b) [サーバ（Server）] ドロップダウン メニューから、ルーティング ノードを選択し、[移動（Go）] をクリックします。

c) CIsco XCP Router サービスが実行されていない場合は、対応するオプション ボタンをオンにし、[開始（Start）] をクリックします。

ステップ 6 ルーティング ノードを除くすべてのクラスタ ノードに対しこの手順を繰り返します。

次の作業

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, （6 ページ）

パーティション イントラドメイン フェデレーション オプションの設定

次の手順では、IM and Presence サービスでパーティション 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 モードを選択する方法について説明します。

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、任意のクラスタ内の IM and Presence サービス パブリッシャ ノードで有効にするだけで設定できます。

注意 フェデレーションの電子メール アドレスは、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た導入ではサポートされません。Skype for Business/Lync/OCS のドメイン間フェデレーション機能を使用する導入では、フェデレーションの電子メール アドレスはドメイン間フェデレーションでもサポートされません。フェデレーションの電子メール アドレスがこれらの展開シナリオのどの展開でも有効になっていないこと、[ドメイン間フェデレーションのために電子メール アドレスの使用を有効化（Enable use of Email Address for Inter-domain Federation）] オプションがクラスタに選択されていないことを確認します。

手順

ステップ 1 [Cisco UnifiedCommunications Manager IM and Presence Administration] ユーザ インターフェースにログインします。[プレゼンス（Presence）]>[設定（Settings）]>[標準設定（Standard Configuration）]

ステップ 2 [LCS/OCS/Lync とのパーティション ドメイン間フェデレーションを有効化（Enable Partitioned Intradomain Federation with LCS/OCS/Lync）] チェックボックスをオンにします。

ステップ 3 警告メッセージに目を通し、[OK] をクリックします。

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。

- ライセンスのない IM and Presence サービス要求の受信者が IM and Presence サービス ドメイン内に存在する場合、[基本ルーティングモード（Basic Routing Mode）（デフォルト）] を選択します。基本ルーティング モードでは、IM and Presence サービスは Microsoft サーバにこれらの受信者の要求をルーティングします。

- ライセンスされていて、有効な Microsoft Lync または Microsoft Office Communicator SIP アドレスが IM and Presence サービス データベースに保存されている要求の受信者が IM and Presence サービス ドメインにある場合は [高度ルーティングモード（Advanced Routing Mode）] を選択します。Cisco Unified Communications Manager が Microsoft サーバが使用する Active Directory からのユーザを同期している場合のみ、[高度ルーティングモード（Advanced Routing Mode）] を選択します。

  （注） Active Directory から同期されたユーザのリストには、すべての Microsoft Lync または Microsoft Office Communicator ユーザが記載されている必要があります。

ステップ 5 [保存（Save）] をクリックします。

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するか、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 サービス ノードの Cisco XCP ルータを再起動する必要があります。Cisco XCP ルータを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインし、[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。適切な IM and Presence サービス ノードをクリックしてスクロール ダウンし、[Cisco XCP ルーター（Cisco XCP Router）] を選択して [再起動（Restart）] をクリックします。

（注） パーティションフェデレーションをイネーブルにするときにSIPプロキシを再起動するように促されます。

次の作業

Microsoft Lync へのスタティック ルートの設定, （7 ページ）

関連トピック

IM and Presence から Microsoft サーバへの要求のルーティング

Microsoft Lync へのスタティック ルートの設定

次の手順では、IM and Presence サービスと Skype for Business/Lync/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ルーティングをイネーブルにするようにスタティック ルートを設定する方法について説明します。各 Microsoft サーバのプレゼンス ドメインの個々のスタティック ルートを追加する必要があります。スタティック ルートには、共通のネクスト ホップ アドレスを設定できます。Microsoft の Server 要求に経路指定に IM and Presence サービスから Microsoft のサーバ要求ルーティングと、基本および高度なルーティング モードに関連するトピックを参照してください。

（注） パーティション イントラドメイン フェデレーションを Microsoft サーバのドメイン間フェデレーション機能と統合している場合、各リモート ドメインの IM and Presence サービスにスタティック ルートを設定します。詳細については、リモート ドメインのスタティック ルートの設定に関するトピックを参照してください。

（注） 各 Microsoft サーバのプレゼンス ドメインに対してこの手順を実行します。

Microsoft サーバのプレゼンス ドメインのスタティック ルートについて、次の点に注意してください。

- Standard Edition Microsoft サーバについて、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。
- フェデレーション トラフィックを IM and Presence サービス クラスタから直接いずれかのフロント エンド Microsoft サーバにルーティングする場合は、スタティック ルートはそのフロント 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。

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、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。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、各 Microsoft サーバのプレゼンス ドメインの追加のバックアップ スタティック ルートを設定できます。

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、任意のクラスタ内の IM and Presence サービス データベース 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 Administration] ユーザ インターフェイスにログインします。[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）] をクリックします。

ステップ 3 ドメインが元に戻るよう [宛先パターン（Destination Pattern）] 値を入力します。たとえば、ドメインが `domaina.com` の場合、宛先パターン値は `.com .domaina` である必要があります

ステップ 4 [ネクストホップ（Next Hop）] フィールドに、Microsoft サーバの IP アドレスを入力します。

ステップ 5 [ルート タイプ（Route Type）] で [domain] を選択します。

（注） ルート タイプのデフォルト設定はユーザです。

ステップ 6 使用するプロトコルに応じて、[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）] の値を設定します。

- TCP の場合：[プロトコルタイプ（Protocol Type）] に [TCP]、[ネクストホップポート（Next Hop Port）] として [5060] を選択します。
- TLS の場合：[プロトコルタイプ（Protocol Type）] に [TLS]、[ネクストホップポート（Next Hop Port）] として [5061] を選択します。

（注） Lync へのスタティック ルートの場合は、TLS ルートを設定する必要があります。OCS へのスタティック ルートの場合は、TLS または TCP を設定できます。

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）] をクリックします。

ステップ 10 ネクスト ホップの Microsoft Lync サーバ IP アドレスとともに、宛先パターンの FQDN を逆順に使用し、追加のスタティック ルートを作成します。たとえば、ドメインが「lyncserver.domaina.com」であれば、[宛先パターン（Destination Pattern）] の値は「.com.domaina.lyncserver」となります。

次の作業

着信アクセス コントロール リストの設定, （9 ページ）

着信アクセス コントロール リストの設定

次の手順では、Skype for Business/Lync/OCS サーバが認証されなくても IM and Presence サービス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。

（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、任意のクラスタ内の IM and Presence サービス パブリッシャ ノードでのみ設定する必要があります。

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

- IM and Presence サービスへのオープン アクセスを許可するには、[すべて（All）] のアドレス パターンのエントリを追加します。
- 特定のネットワーク ドメインから IM and Presence サービスへのアクセスを許可する場合は、アドレス パターンが特定のドメインと一致するエントリを追加します。たとえば、foo.com DNS ドメイン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 サービスへのアクセスを許可するには、IP アドレスと一致するアドレス パターンとこれらのサーバの FQDN を持つ ACL エントリを追加します。各サーバで IP アドレスと FQDN の 2 つの ACL エントリを作成する必要があります。たとえば、サーバ ocs1.foo.com（10.1.10.100）からのアクセスを許可するには、1 つの ACL エントリとして **ocs1.foo.com** と入力し、別の ACL エントリの宛先パターンとして **10.1.10.100** と入力します。

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、IM and Presence サービスへのアクセスを特定の Microsoft サーバ FQDN または IP アドレスのみに制限する場合、次のエンティティの ACL エントリを追加する必要があります。

- 各 Microsoft サーバ Enterprise Edition フロント エンドまたは Standard Edition サーバ
- Microsoft の各サーバ プール FQDN（Enterprise Edition のみ）
- Gateway Expressway FQDN（チャット + 通話シナリオのみ）

サーバの FQDN を使用してアクセスを制限する場合は、フロント エンド サーバまたはプールと同じ IP アドレスに解決する他の DNS レコードの ACL エントリを追加する必要があります。たとえば、admin.lync.com などのいずれかの Lync のフロント エンド サーバと同じ IP アドレスに解決する Lync コントロール パネルにアクセスする DNS レコードを Lync サーバに作成できます。

注意 特定のサーバの FQDN または ACL エントリの IP アドレスを入力する場合、説明通りのすべての必要な ACL エントリの作成に失敗すると、Lync 2013 クライアントの安定性の問題が生じる場合があります。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[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）] をクリックします。

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

ステップ 4 [アドレス パターン（Address Pattern）] フィールドにアドレス パターンを入力します。次の選択肢があります。

- IM and Presence サービスへのオープン アクセスを許可するには、「Allow from all」と入力します。

- 特定のネットワーク ドメイン名を入力します（例：Allow from foo.com）。
- 特定の IP アドレスを入力します（例：Allow from 10.1.10.100）。
- 特定の FQDN を入力します（例：Allow from admin.lync.com）。

（注） アドレス パターンとして「Allow from All」を入力しない場合、サーバの IP アドレスとサーバの FQDN の少なくとも 2 つの ACL エントリを作成する必要があります。ドメイン名の入力はオプションです。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 以下を実行して SIP プロキシを再起動します。

a) [プレゼンス（Presence）] > [ルーティング（Routing）] > [設定（Settings）] を選択します。

b) [すべてのプロキシサービスのリスタート（Restart All Proxy Services）] ボタンをクリックします。

次の作業

アプリケーション リスナー ポートを設定します。，（11 ページ）

TLS 暗号化の設定

IM and Presence サービスと Skype for Business/Lync/OCS の間で TLS 暗号化を設定するには、この項の手順を完了する必要があります。TLS暗号化は、Lync サーバを持つパーティション イントラドメイン フェデレーションに必須です。

（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、任意のクラスタ内の IM and Presence サービス 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 ポートを設定します。

サーバ認証とピア認証の両方の [デフォルト Cisco SIP Proxy TLS リスナー（Default Cisco SIP Proxy TLS Listener）] 値を変更する必要があります。IM and Presence サービスは、デフォルトではポート 5062 でピア（相互）TLS 認証を実行します。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し、サーバ TLS 認証ポート値を 5062 に設定する必要があります。

手順

ステップ 1 [Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。[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 表示されるポップアップ ウィンドウで、[保存（Save）] をクリックし、[OK] をクリックします。

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 表示されるダイアログボックスで [Save（保存）] をクリックし、[OK] をクリックします。

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 **5063** ～ **5062** のポート値を変更します。

ステップ 13 [保存（Save）] をクリックします。

ステップ 14 クラスタのすべての IM and Presence サービス ノードで SIP Proxy サービスを再起動します。SIP プロキシ サービスを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインし、[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, （12 ページ）

関連トピック

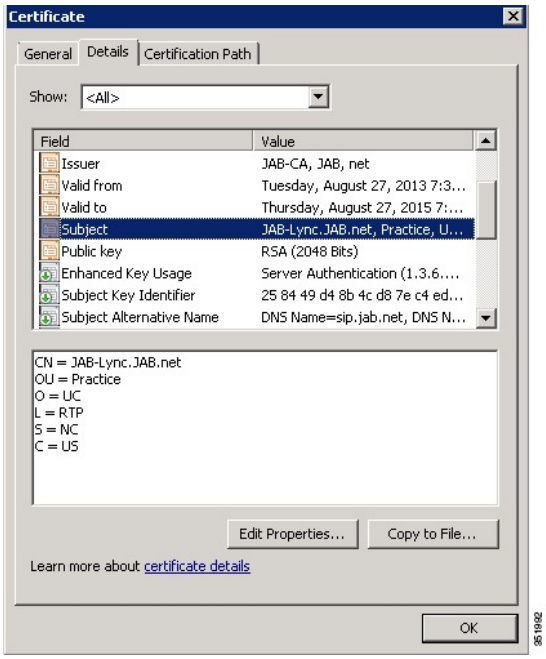
統合のトラブルシューティング

TLS ピア サブジェクトの設定

ピア TLS 認証の場合、IM and Presence サービス 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。[Cisco Unified IM and Presence Administration] ユーザ インターフェイスを使用して、件名 CN をこのリストに追加します。

[TLS ピア サブジェクト（TLS Peer Subject）] リストには件名 CN だけを含めます。[TLS ピア サブジェクト（TLS Peer Subject）] リストに [サブジェクト名の別名（Subject Alternate Name）] エントリを含めないでください。次の図は、件名 CN が強調表示されている件名 CN 証明書の例を示します。

図 *1*：件名共通名の証明書



パーティションイントラドメインフェデレーションの場合は、展開している次のエンティティのいずれか用に TLS ピア サブジェクトを追加します。

- 各 Skype for Business/Lync/OCS Enterprise Edition フロント エンド サーバまたは Standard Edition サーバ
- 各 Skype for Business/Lync/OCS プールの完全修飾ドメイン名（FQDN）（Enterprise Edition のみ）
- Expressway Gateway FQDN（チャット + 通話シナリオの場合のみ）

手順

ステップ 1 [Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。[システム（System）] > [セキュリティ（Security）] > [TLS ピア サブジェクト（TLS Peer Subjects）] を選択します。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 ピア サブジェクト名を入力します。

- Microsoft サーバの Enterprise Edition フロント エンドまたは Standard Edition サーバには、サーバの FQDN を入力します。
- Microsoft サーバ プールの完全修飾ドメイン名（FQDN）には、IM and Presence サービスに提示する証明書の件名 CN を入力します。
- Expressway Gateway の FQDN を入力します（チャット + 通話シナリオの場合のみ）。

ステップ 4 [説明（Description）] フィールドに、サブジェクトの説明を入力します（例：OCS Server）。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 クラスタのすべての IM and Presence サービス ノードで Cisco SIP Proxy サービスを再起動します。Cisco SIP プロキシ サービスを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインし、[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。[CUCM IM and Presence サーバ（CUCM IM and Presence Server）] をクリックし、[SIP プロキシ(SIP Proxy）] を選択して [再起動（Restart）] をクリックします。

次の作業

ピア認証 TLS コンテキストの設定, （14 ページ）

関連トピック

統合のトラブルシューティング

ピア認証 TLS コンテキストの設定

IM and Presence サービス および Skype for Business/Lync/OCS 間の TLS 暗号化をサポートするには、IM and Presence サービス 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。

（注） Microsoft Lync は EC 暗号方式をサポートしていません。EC 暗号方式を選択する場合は、非 EC 暗号方式のみ、または EC 暗号方式と非 EC 暗号方式の混合のいずれかを選択する必要があります。EC 暗号方式は、単独では選択できません。

（注） `Default_Cisco_SIP_Proxy_Peer_Auth_TLS_Context` は、追加のより強力な暗号方式の選択をサポートします。必要な設定に基づいて適切な暗号方式を選択できます。イントラドメイン フェデレーションを設定する前に、選択した暗号リストがピアのサポートされている暗号方式と一致することを確認する必要があります。

手順

ステップ 1 [Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。[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）] をクリックします。

ステップ 3 デフォルト Cisco UP SIP プロキシ ピア認証 TLS コンテキスト用のリンクをクリックします。

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

ステップ 5 [TLS 暗号化マッピング（TLS Cipher Mapping）] 領域の [利用可能な TLS 暗号化（Available TLS Ciphers）] リストで、すべての暗号を選択し、[右に移動（Move Right）] 矢印をクリックし、これらの暗号を [選択した TLS 暗号化（Selected TLS Ciphers）] リストに移動します。

ステップ 6 [TLS ピア サブジェクト マッピング（TLS peer Subject Mapping）] 領域の [利用可能な TLS ピア サブジェクト（Available TLS Peer Subjects）] リストで、TLS ピア サブジェクトの設定, （12 ページ） で設定した TLS ピア サブジェクトを選択し、[Move Right（右に移動）] 矢印をクリックし、[Selected TLS Peer Subjects（選択された TLS ピア サブジェクト）] リストに移動します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 クラスタのすべての IM and Presence サービス ノードで Cisco SIP Proxy サービスを再起動します。SIP プロキシ サービスを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインし、[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。CUCM IM and Presence サービス サーバをクリックし、[Cisco SIP Proxy] を選択して [リスタート（Restart）] をクリックします。

次の作業

認証局のルート証明書のインポート, （15 ページ）

関連トピック

統合のトラブルシューティング

認証局のルート証明書のインポート

通常、すべての Skype for Business 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 サービス証明書も、Microsoft サーバと同じ認証局によって署名する必要があります。IM and Presence サービスが Microsoft サーバ CA で署名された証明書を使用し、その同じ CA で署名された Microsoft サーバ証明書を承認するには、CA のルート証明書を IM and Presence サービス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 [Cisco Unified IM and Presence OS Administration] ユーザ インターフェイスにログインします。[セキュリティ（Security）] > [証明書管理（Certificate Management）] を選択します。

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

ステップ 3 [証明書の名前（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 [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（わかりやすい名前）を入力します。

ステップ 5 [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 6 [アップロード（Upload）] をクリックし、証明書を IM and Presence サービス ノードにアップロードします。

ステップ 7 クラスタのすべての IM and Presence サービス ノードで Cisco SIP Proxy サービスを再起動します。Cisco SIP プロキシ サービスを再起動するには、[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインし、[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。CUCM IM and Presence サービス サーバをクリックし、[Cisco SIP Proxy] を選択して [リスタート（Restart）] をクリックします。

次の作業

IM and Presence サービスの証明書署名要求の生成, （16 ページ）

IM and Presence サービスの証明書署名要求の生成

IM and Presence サービス証明書が Skype for Business により使用される同じ認証局（CA）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。

1. IM and Presence サービス証明書署名付き要求（CSR）の生成
2. CA 署名付き証明書を IM and Presence サービスにアップロードします。

次の手順では、IM and Presence サービスから 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 サービス CSR のサイズは、2048 ビットです。

手順

ステップ 1 [Cisco Unified IM and Presence Administration] ユーザ インターフェイスにログインします。IM and Presence サービスで、[セキュリティ（Security）] > [証明書管理（Certificate Management）]を選択します。

ステップ 2 [CSR を作成（Generate CSR）] をクリックします。

ステップ 3 [証明書目的（Certificate Purpose）] ドロップダウン リストで、cup を選択します。

ステップ 4 [CSR を作成（Generate CSR）] をクリックします。

ステップ 5 [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 6 [CSR をダウンロード（Download CSR）] をクリックします。

ステップ 7 [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 8 [CSR をダウンロード（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 9 証明書がダウンロードされたら、[閉じる（Close）] を選択します。

次の作業

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。詳細は、CA からの署名付き証明書のインポートを参照してください。

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 サービス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 サービス から CSR を生成し、ダウンロードします。IM and Presence サービスの証明書署名要求の生成, （16 ページ）を参照してください。

手順

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

ステップ 2 [証明書をアップロード（Upload Certificate）] をクリックすると [証明書/証明書チェーンをアップロード（Upload Certificate/Certificate chain）] ダイアログボックスが開きます。

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 [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（わかりやすい名前）を入力します。

ステップ 5 [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 6 [アップロード（Upload）] をクリックし、証明書を IM and Presence サービス ノードにアップロードします。

ステップ 7 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 Cisco SIP Proxy サービスを再起動します。Cisco SIP プロキシ サービスを再起動するには、[Cisco Unified IM and Presence Servicceability] ユーザ インターフェイスにログインします。[ツール（Tools）] > [コントロール センターの機能サービス（Control Center – Feature Services）] を選択します。Cisco Unified IM and Presence サービス サーバをクリックし、[Cisco SIP Proxy] を選択して [リスタート（Restart）] をクリックします。

次の作業

Lync によるチャット + 通話フェデレーションの場合、Expressway Gateway の設定, （18 ページ）

それ以外のチャット専用の場合は、次の章のいずれかに移動します。

- パーティション イントラドメイン フェデレーション用 Microsoft Lync の設定
- Microsoft Office Communications Server for Partitioned Intradomain Federation の設定

Expressway Gateway の設定

チャット + 通話の展開のみ。Expressway Gateway で、Microsoft の相互運用性を設定し、SIP ブローカを有効にします。Expressway Gateway の構成については、次の URL で『*Cisco Expressway and Microsoft Lync Deployment Guide*』を参照してください。

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

（注） チャットのみの展開の場合は、Expressway Gateway を展開する必要はありません。

次の作業

パーティション イントラドメイン フェデレーション用 Microsoft Lync の設定