XMPP フェデレーションに使用するセキュリティ証明書の設定

XMPP フェデレーションに使用するセキュリティ証明書の設定

XMPP フェデレーション用のセキュリティを設定するためには、以下のような操作を行う必要があります。

1. cup-xmpp-s2s 証明書を生成する前に、すべてのローカル ドメインがシステムで作成および設定されていることを確認し、必要に応じて、見つからないローカル ドメインを手動で作成します。
2. 次のいずれかのタイプの証明書を作成します。
   - XMPP フェデレーション用の自己署名付きの単一サーバ証明書
   - XMPP フェデレーション用の CA 署名付きの単一サーバ証明書またはマルチサーバ証明書
3. ルート CA 証明書をインポートします。

   まだ信頼していない CA を使用するエンタープライズとのフェデレーションを新たに設定するたびに、この操作を繰り返します。同様に、フェデレーションを新たに設定するエンタープラ

イズが自己署名証明書を使用している場合もこの操作を行う必要があります。この場合、ルート CA 証明書の代わりに自己署名証明書がアップロードされます。

XMPP フェデレーションのローカル ドメイン検証

すべてのローカル ドメインは、生成された cup-xmpp-s2s の証明書に含まれている必要があります。cup-xmpp-s2s 証明書を生成する前に、すべてのローカル ドメインが設定されていて、[ドメイン（Domains）] ウィンドウに表示されることを確認します。計画に含まれているドメインを手動で追加しますが、ローカル ドメインのリストには表示されません。たとえば、ユーザが割り当てられていないドメインは、通常の場合ドメインのリストに表示されません。

[Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインし、[プレゼンス（Presence）] > [ドメイン（Domains）]を選択します。

すべてのドメインがシステムで作成されていることを確認した後は、XMPP フェデレーション用の自己署名証明書または CA 署名付き証明書を使用して、cup-xmpp-s2s 証明書を作成する手順に進むことができます。フェデレーション用の電子メール アドレスが有効な場合は、すべての電子メール ドメインも証明書に含める必要があります。

ローカル ドメインを追加、更新または削除して、cup-xmpp-s2s 証明書を再生成する場合は、Cisco XCP XMPP Federation Connection Manager サービスを再起動する必要があります。この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 Service）] を選択します。

関連トピック

電子メール ドメインを追加または更新する
XMPP フェデレーションに自己署名証明書を使用する, （3 ページ）
XMPP フェデレーションへの CA 署名付き証明書の使用, （3 ページ）
電子メール ドメインを表示する

マルチサーバ証明書の概要

IM and Presence サービスは、tomcat、cup-xmpp、および cup-xmpp-s2s の証明のために、マルチサーバ SAN ベースの証明書をサポートしています。適切な証明書署名要求（CSR）を生成するために、シングルサーバまたはマルチサーバ配布を選択できます。作成された署名付きマルチサーバ証明書と関連付けられたその一連の署名証明書は、クラスタ内の個々のサーバにマルチサーバ証明書をアップロードする際に、クラスタ内の他のサーバに自動的に配布されます。マルチサーバ証明書の詳細については、『*Release Notes for Cisco Unified Communications Manager Release 10.5(1)*』の新機能と変更された機能に関する章を参照してください。

XMPP フェデレーションに自己署名証明書を使用する

ここでは、XMPP フェデレーションに自己署名証明書を使用する方法について説明します。CA 署名付き証明書の使用方法については、XMPP フェデレーションへの CA 署名付き証明書の使用，（3 ページ）を参照してください。

手順

ステップ 1 [Cisco Unified IM and Presence Operating System Administration] ユーザ インターフェイスにログインします。[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 [自己署名付きを生成（Generate Self-signed）] をクリックします。

ステップ 3 [証明書の用途（Certificate Purpose）] ドロップダウン リストから、[cup-xmpp-s2s] を選択して、[生成（Generate）] をクリックします。

ステップ 4 Cisco XCP XMPP Federation Connection Manager サービスを再起動します。[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[ツール（Tools）] > [コントロール センタ - ネットワーク サービス（Control Center - Network Services）] を選択して、このサービスを再起動します。

ステップ 5 証明書をダウンロードして別のエンタープライズに送信して、XMPP サーバの信頼できる証明書として追加できます。これには、IM and Presence サービス ノードまたは別の XMPP サーバなどがあります。

次の作業

XMPP フェデレーションへの CA 署名付き証明書の使用，（3 ページ）

XMPP フェデレーションへの CA 署名付き証明書の使用

ここでは、CA 署名付き証明書を使用する方法について説明します。自己署名付き証明書の使用方法については、XMPP フェデレーションに自己署名証明書を使用する，（3 ページ）を参照してください。

XMPP フェデレーションの証明書署名要求を生成する

ここでは、Microsoft Certificate Services CA の証明書署名要求（CSR）を生成する方法について説明します。

（注） この手順では Microsoft Certificate Services CA の CSR を生成しますが、任意の認証局の証明書を要求する場合は、CSR を生成する手順（手順 1 ～ 3）が適用されます。

手順

ステップ 1 [Cisco Unified IM and Presence Operating System Administration] ユーザ インターフェイスにログインします。[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 CSR を生成するには、次の手順を実行します。

a) [CSR の作成（Generate CSR）] をクリックします。

b) [証明書の用途（Certificate Purpose）] ドロップダウン リストから、証明書名に [cup-xmpp-s2s] を選択します。

c) 配信用には、単一署名された証明書を生成するローカル サーバ、またはマルチサーバ証明書を生成するマルチサーバ（SAN）の FQDN を選択します。

（注） 両方のディストリビューション オプションでは、すべての既存のドメイン、電子メール ドメインおよび [Cisco Unified IM and Presence Administration] ユーザ インターフェースで設定されたグループ チャットのサーバ エイリアスは、生成された CSR に自動的に含まれます。[Multi-server (SAN)（マルチサーバ（SAN））] オプションを選択した場合、各 IM and Presence サービス ノードのホスト名または FQDN は、生成された CSR に追加されます。マルチサーバ証明書の詳細については、『*Release Notes for Cisco Unified Communications Manager Release 10.5(1)*』の新機能と変更された機能に関する章を参照してください。

d) [生成（Generate）] をクリックします。

（注） [Multi-server（SAN）（マルチサーバ（SAN））] を選択した場合、CSR はクラスタの他のすべての IM and Presence サービス ノードのファイル システムにコピーされます。

e) [閉じる（Close）] をクリックし、メインの証明書ウィンドウに戻ります。

ステップ 3 `.csr` ファイルをローカル マシンにダウンロードするには：

a) [CSR をダウンロード（Download CSR）] をクリックします。

b) [証明書目的（Certificate Purpose）] ドロップダウン メニューから [cup-xmpp-s2s] を選択します。

c) [CSR をダウンロード（Download CSR）] をクリックして、そのファイルをローカル マシンにダウンロードします。

ステップ 4 テキスト エディタを使用して `cup-xmpp-s2s.csr` ファイルを開きます。

ステップ 5 CSR ファイルの内容をコピーします。
次の行から、

- BEGIN CERTIFICATE REQUEST

次の行までの情報をすべてコピーします。

END CERTIFICATE REQUEST -

ステップ 6 インターネット ブラウザで、CA サーバを参照します。たとえば、次のように指定します。`http://<name of your Issuing CA Server>/certsrv`。

ステップ 7 [証明書を要求する（Request a certificate）] をクリックします。

ステップ 8 [証明書の要求の詳細設定（Advanced certificate request）] をクリックします。

ステップ 9 [ベース 64 エンコード CMC または PKCS #10 ファイルを使用して証明書要求を送信するか、ベース 64 エンコード PKCS #7 ファイルを使用して更新要求を送信する（Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file）] をクリックします。

ステップ 10 手順 5 でコピーした CSR ファイルの内容を [保存した要求（Saved Request）] フィールドに貼り付けます。

ステップ 11 [送信（Submit）] をクリックします。

ステップ 12 インターネット ブラウザで、次の URL に戻ります。 `http://<name of your Issuing CA Server>/certsrv`

ステップ 13 [保留中の証明書の要求の状態（View the status of a pending certificate request）] をクリックします。

ステップ 14 前の項で発行した証明書の要求をクリックします。

ステップ 15 [ベース 64 エンコード（Base 64 encoded）] をクリックします。

ステップ 16 [証明書をダウンロード（Download Certificate）] をクリックします。

ステップ 17 証明書をローカル マシンに保存します。

a) 証明書ファイル名 `cup-xmpp-s2s.pem` を指定します。

b) 証明書を**セキュリティ証明書**として保存します。

次の作業

XMPP フェデレーションへの CA 署名付き証明書をアップロードする，（5 ページ）

トラブルシューティングのヒント

- IM and Presence サービスのサポートされるドメインのリストが変更される場合は、新しいドメイン リストを反映するように cup-xmpp-s2s 証明書を再生成する必要があります。

XMPP フェデレーションへの CA 署名付き証明書をアップロードする

はじめる前に

XMPP フェデレーションの証明書署名要求を生成する，（3 ページ）の手順を実行します。

手順

ステップ 1 [Cisco Unified IM and Presence Operating System Administration] ユーザ インターフェイスにログインします。[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 証明書名に [cup-xmpp-s2s] を選択します。

ステップ 4 ローカル マシンに保存した CA 署名付き証明書の場所を参照します。

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

（注） マルチサーバの SAN ベースの証明書を生成した場合は、クラスタ内の任意の IM and Presence サービス ノードへこれをアップロードできます。これを実行すると、結果として署名証明書署名されたマルチ・サーバ証明書と関連チェーンがクラスタの個々のサーバがデバイスと証明書のアップロードのクラスタ内の他のサーバに自動的に配布されます。自己署名証明書がノードのいずれかにある場合、新しい複数サーバの証明書によって上書きされます。マルチサーバ証明書の詳細については、『*Release Notes for Cisco Unified Communications Manager Release 10.5(1)*』の新機能と変更された機能に関する章を参照してください。

ステップ 6 Cisco XMPP Federation Connection Manager サービスを再起動します。[Cisco Unified IM and Presence Serviceability] ユーザ インターフェイスにログインします。[ツール（Tools）] > [コントロール センタ - ネットワーク サービス（Control Center - Network Services）] を選択して、このサービスを再起動します。

（注） マルチサーバの証明書をアップロードするには、クラスタ内の**すべて**の IM and Presence サービス ノードで XCP ルータ サービスを再起動する必要があります。

次の作業

同じクラスタ内のノード間でサービスアビリティ用のクロス ナビゲーションをサポートするために、IM and Presence サービスと Cisco Unified Communications Manager の間の Cisco Tomcat サービス信頼ストアが自動的に同期されます。

IM and Presence サービスまたは Cisco Unified Communications Manager のいずれかで元の自己署名信頼証明書を置き換えるためにCA署名付き証明書が生成されても、元の証明書は、ノードのサービス信頼ストアで保持されます。サービス信頼ストアに元の自己署名証明書を残しても、それらを表すサービスがないため、問題になりません。ただし、これらの証明書は削除できますが、削除は IM and Presence サービスと Cisco Unified Communications Manager の両方で実行する必要があります。

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』の該当リリースの第 II 部の第 9 章「Security Configuration on IM and Presence Service」にある「Delete Self-Signed Trust Certificates」セクションを参照してください。

XMPP フェデレーションのルート CA 証明書をインポートする

（注） ここでは、cup-xmpp-s2s 信頼証明書を IM and Presence サービスに手動でアップロードする方法について説明します。また、Certificate Import Tool を使用して、cup-xmpp-s2s 信頼証明書を自動的にアップロードすることもできます。証明書のインポート ツール、ログインおよびプレゼンス管理**ユーザ インターフェイスに Cisco Unified** CM IM にアクセスする。[システム（System）] > [セキュリティ（Security）] > [証明書インポート ツール（Certificate Import Tool）] を選択し、このツールを使用する手順を記載するオンライン ヘルプを参照してください。

IM and Presence サービスとエンタープライズのフェデレーションを行い、共通の信頼できる認証局（CA）がエンタープライズの証明書に署名する場合、CA のルート証明書を IM and Presence サービス ノードにアップロードする必要があります。

共通の信頼できる CA が署名した証明書ではなく、自己署名証明書を使用するエンタープライズと IM and Presence サービスのフェデレーションを行う場合、この手順を使用して自己署名証明書をアップロードできます。

はじめる前に

ルート CA 証明書をダウンロードし、ローカル マシンに保存します。

手順

ステップ 1 [Cisco Unified IM and Presence Operating System Administration] ユーザ インターフェイスにログインします。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 [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）] をクリックします。

ステップ 3 証明書名に [cup-xmpp-trust] を選択します。

（注） ルート名のフィールドは空白のままにしておきます。

ステップ 4 [参照（Browse）] をクリック、以前にダウンロードしてローカル マシンに保存したルート CA 証明書の場所を参照します。

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

（注） まだ信頼していない CA を使用するエンタープライズとのフェデレーションを新たに設定するたびに、この操作を繰り返します。同様に、フェデレーションを新たに設定するエンタープライズが自己署名証明書を使用している場合もこの操作を行う必要があります。この場合、ルート CA 証明書の代わりに自己署名証明書がアップロードされます。

トラブルシューティングのヒント

信頼証明書が自己署名の場合、XMPP フェデレーションのセキュリティ設定ウィンドウで[クライアント側の証明書が必要（Require client side certificates）]パラメータをオンにすることはできません。