Microsoft Office Communications Server for Partitioned Intradomain Federation の設定

パーティション イントラドメイン フェデレーションの Microsoft Office Communications サーバの設定は、Microsoft Office Communications Server (OCS) 2007 R2 にのみ適用されます。

OCS サーバのドメインの確認

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、Microsoft LCS サーバに一致するドメインが設定されていることと、IM and Presence サービス クラスタにすべてのノードがあることを確認します。

Cisco Unified CM IM and Presence Administration ユーザ インターフェイスを使用して、IM and Presence サービスに設定されたローカル ドメインと、外部サーバに設定されたシステム管理ドメインを確認します。

OCS サーバでのポート 5060/5061 の有効化

IM and Presence サービス および OCS との間の SIP トラフィックに暗号化されていない TCP 接続を使用する場合は、OCS サーバを SIP TCP ポート 5060 でリッスンするように設定します。フェデレーテッド TLS 接続に、TLS ポート 5061 でリッスンするように OCS サーバを設定します。

（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 スタンダード エディションまたは 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 または 5061 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 アドレス値（IP Address Value）] に [すべて（All）] を選択します。

ステップ 6 輸送およびポート値を入力します。

- TCP の場合、[トランスポート（Transport）] に TCP、[ポート（Port）] に 5060 を入力します。
- TLS の場合、[トランスポート（Transport）] に TLS、[ポート（Port）] に 5061 を入力します。

ステップ 7 [OK] をクリックして、[接続を追加（Add Connection）] ウィンドウを閉じます。これで、ポート値が [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 サービスを指すように OCS サーバのスタティック ルートを設定します。

関連トピック

統合のトラブルシューティング

Microsoft OCS サーバ コンフィギュレーション タスク リストへのフェデレーテッド リンク

次の表では、IM and Presence サービスと Microsoft OCS サーバ間のフェデレーション リンクを設定する手順の概要を示します。

Access Edge サーバまたは Cisco Adaptive Security Appliance なしで IM and Presence サービスから OCS に直接フェデレーションを使用している場合は、OCS サーバの各ドメインで TLS または TCP のスタティック 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 サービス ノードをポイントします。Cisco Adaptive Security Appliance または Microsoft Access Edge は必要ではありません。

- Standard Edition では Standard Edition サーバのスタティック ルートを設定する必要があります。
- Enterprise Edition では、すべてのプールにスタティック ルートを設定する必要があります。

表 *1*：*Microsoft OCS* サーバへのフェデレーション リンクのエンドツーエンド設定のタスク リスト

手順	説明
IM and Presence サービスのスタティック ルートの設定	TLS または TCP がサポートされています。 TLS では、[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）] の番号として [5061] を選択します。 TCP では、[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）] の番号として [5060] を選択します。

手順	説明
OCS での IM and Presence サービスのスタティック ルートの設定	TLS または TCP がサポートされています。 TLS の場合、スタティック ルート ポートは 5061 になります。 TCP の場合、スタティック ルート ポートは 5060 になります。 **重要** OCS のスタティック ルートとともに TLS を使用する場合は、IM and Presence サービス ノードの IP アドレスでなく FQDN を指定する必要があります。 ピア認証リスナー ポートを 5061 に設定し、サーバ承認リスナー ポートを変更します。 **Cisco Unified CM IM and Presence Administration** にログインし、[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。 • 必ずピア認証リスナー ポートを 5061 にします。 • サーバ認証リスナー ポートが 5061 に設定されている場合は、別の値（5063）に変更する必要があります。
IM and Presence サービス用のホスト認証エントリを設定します。	この手順は、TLS および TCP に適用されます。 TLS では、IM and Presence サービス ノードそれぞれについて、1 つのエントリにIM and Presence サービス ノードの IP アドレスを使用し、2 つ目のエントリに IM and Presence サービス FQDN を使用して、2 つのホスト認証エントリを追加する必要があります。 TCP の場合、IM and Presence サービス IP アドレスを使用する 1 つのホスト認証エントリのみを各 IM and Presence サービス ノードに追加する必要があります。

手順	説明
OCS での証明書の設定	この手順は TLS の場合だけです。 CA ルート証明書および OCS の署名付き証明書を取得するには、次の手順を実行します。 • CA 証明書チェーンをダウンロードおよびインストールします。 • CA サーバの証明書を要求します。 • CA サーバから証明書をダウンロードします。 OCS の[フロント エンド サーバ プロパティ（Front End Server Properties）] で、OCS のポート 5061 で TLS リスナーが設定されていることを確認します（トランスポートは MTLS または TLS の場合もあります）。 [OCS フロント エンド サーバのプロパティ（OCS Front End Server Properties）] で、[証明書（Certificates）] タブを選択し、[証明書の選択（Select Certificate）] をクリックして、OCS 署名証明書を選択します。
FIPS（SSLv3 よりも、TLSv1）を使用するように OCS を設定し CA ルート証明書をインポートします。	この手順は TLS の場合だけです。 1 OCS のローカル セキュリティ設定を開きます。 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。 3 [セキュリティ オプション（Security Options）] を選択します。 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。 5 セキュリティ設定を有効にします。 6 [OK] をクリックします。 （注） 有効にするには、OCS を再起動する必要があります。 7 IM and Presence サービス証明書に署名した CA の CA ルート証明書をインポートします。証明書スナップインを使用して OCS の信頼ストアに CA ルート証明書をインポートします。

手順	説明
IM and Presence サービス証明書の設定	この手順は TLS の場合だけです。 IM and Presence サービスに OCS サーバ証明書に署名した CA のルート証明書をアップロードします。また、IM and Presence サービス用の CSR を生成し、CA によって署名されるようにします。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。 その後、OCS サーバの IM and Presence サービスで TLS ピア サブジェクトを追加します。詳細な手順については、証明書のセットアップに関するトピックを参照してください。

IM and Presence サービスをポイントする OCS のスタティック ルートの設定

ダイレクト フェデレーション用に OCS が IM and Presence サービスに要求をルーティングできるようにするには、各 IM and Presence サービス ドメインについて OCS サーバで TLS または TCP のスタティック 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 サービス ノードをポイントします。

（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 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）] をクリックします。

ステップ 5 foo.com など、IM and Presence サービス ノードのドメインを入力します。

ステップ 6 [電話 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 ネクスト ホップ トランスポート、ポート、IP アドレス/FQDN 値を設定します。

- TCP の場合は、[ネクスト ホップ トランスポート（Next Hop Transport）] 値に [TCP] を選択し、[ネクスト ホップ ポート（Next Hop Port）] 値に **5060** を入力します。ネクスト ホップ IP アドレスとして IM and Presence サービス ノードの IP アドレスを入力します。

- TLS の場合は、[ネクスト ホップ トランスポート（Next Hop Transport）] 値に [TLS] を選択し、[ネクスト ホップ ポート（Next Hop Port）] 値に **5061** を入力します。FQDN として IM and Presence サービス ノードの IP アドレスを入力します。

（注）
- TLS のスタティック ルートに使用するポートは、IM and Presence サービス ノードで設定されたピア認証のリスナー ポートに一致する必要があります。
- FQDN は OCS サーバで解決可能である必要があります。FQDN が IM and Presence サービス ノードの IP アドレスに解決されることを確認します。

ステップ 8 [要求 URI のホストを置換（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 9 [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 10 [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

『Interdomain Federation for IM and Presence Service on Cisco Unified Communcations Manager guide』の「Verify Peer Authentication Listener」を参照してください。

OCS での IM and Presence サービスのホスト認証の追加

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

TCP の場合、IM and Presence サービス IP アドレスを使用する 1 つのホスト認証エントリのみを各 IM and Presence サービス ノードに追加する必要があります。

OCS とIM and Presence サービス間の TLS 暗号化を設定する場合、次のように各 IM and Presence サービス ノードに 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 サービス ノードの FQDN を含める必要があります。
- 2 つ目のエントリには、IM and Presence サービス ノードの IP アドレスを含める必要があります。

TLS 暗号化を設定しない場合は、IM and Presence サービス ノードに 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 サービス ノードの 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 プロパティ（Front End Properties）] を選択します。

ステップ 4 [ホスト認証（Host Authorization）] タブを選択し、[追加（Add）] をクリックします。

ステップ 5 FQDN を入力している場合、[FQDN] を選択して、IM and Presence サービス ノードの FQDN を入力します。たとえば、imp1.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 サービス ノードの 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 [発信のみ（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 [サーバとしてのスロットル（Throttle as Server）] チェックボックスをオンにします。

ステップ 9 [認証付きとして処理（Treat as Authenticated）] チェックボックスをオンにします。

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 ノードごとに手順 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, （8 ページ）

関連トピック

統合のトラブルシューティング

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 のフロント エンド サーバの FQDN を右クリックし、[スタート（Start）] > [フロント エンド サービス（Front End Service）] > [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

TLS 暗号化の設定

IM and Presence サービスと 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 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, （8 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 サービス 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] をクリックします。

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, （10 ページ）

関連トピック

統合のトラブルシューティング

TLS 相互認証の OCS での設定

IM and Presence サービスおよび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 [一般（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 [トランスポート（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、[接続を編集（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] をクリックして、[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, （11 ページ）

関連トピック

統合のトラブルシューティング

認証局ルート証明書の OCS へのインストール

IM and Presence サービス 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 サービス ノードで同じ 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 サービス証明書に署名した 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 サービスが同じ 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、[スタート（Start）] > [実行（Run）] を選択します。

ステップ 2 `mmc` と入力し、[OK] をクリックします。

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 [利用可能なスタンドアロン スナップイン（Available Standalone Snap-ins）] リストで、[Certificates（証明書）] を選択し、[Add（追加）] 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）] をクリックします。

ステップ 7 [コンピュータを選択（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中のコンピュータ）（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）] をクリックしてから、[OK] をクリックします。

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）] をクリックします。

ステップ 13 [インポート（Import）] ウィザードで、[次へ（Next）] をクリックします。

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）] をクリックします。

ステップ 16 [Next] をクリックします。

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）] をクリックし、[終了（Finish）] をクリックします。

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, （13 ページ）

関連トピック

統合のトラブルシューティング
『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 サービスと 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、[スタート（Start）] > [実行（Run）] を選択します。

ステップ 2 `mmc` と入力し、[OK] をクリックします。

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 [利用可能なスタンドアロン 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）] をクリックします。

ステップ 7 [コンピュータを選択（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中のコンピュータ）（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）] をクリックしてから、[OK] をクリックします。

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 [パーソナル（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 [サーバとクライアントの認証の証明書（Server and 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

OCS サーバの認証局から署名付き証明書の要求, （14 ページ）

関連トピック

統合のトラブルシューティング

OCS サーバの認証局から署名付き証明書の要求

この項では、Microsoft Office Communicator Server（OCS）に署名入り証明書をインストールし、TLS ネゴシエーションのためにインストールした証明書を選択する方法について説明します。

（注） このトピックの手順は、OCS 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 サービスと 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 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』

OCS サーバで署名付き証明書をインストールします。

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、[スタート（Start）] > [実行（Run）] を選択します。

ステップ 2 mmc と入力し、[OK] をクリックします。

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 [利用可能なスタンドアロン 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）] をクリックします。

ステップ 7 [コンピュータを選択（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中のコンピュータ）（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）] をクリックしてから、[OK] をクリックします。

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）] をクリックします。

ステップ 13 [インポート（Import）] ウィザードで、[次へ（Next）] をクリックします。

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）] をクリックします。

ステップ 16 [Next] をクリックします。

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）] をクリックし、[終了（Finish）] をクリックします。

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, （17 ページ）

関連トピック

統合のトラブルシューティング

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 サービス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 スタンダード エディション 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、[証明書を選択（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] をクリックして、[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, （8 ページ）

関連トピック

統合のトラブルシューティング