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

パーティション イントラドメイン フェデレーション用の Microsoft Lync を設定するには、次の手順を記載されている順序で実行します。設定が完了したら、Lync サーバでサービスを再起動する必要があります。

（注）

Lync とのパーティション イントラドメイン フェデレーションの TLS を設定する必要があります。Lync では TCP はサポートされません。

Lync 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 Lync サーバに一致するプレゼンス 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 インターフェイスで [プレゼンス（Presence）] > [ドメイン（Domains）] > [検索（Find）] を選択し、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。

Lync フェデレーション設定タスク フロー

次の手順を実行して、パーティション イントラドメイン フェデレーション用に Microsoft Lync をセットアップします。この設定では、チャット専用の展開とチャット+通話の展開の両方をサポートしています。

はじめる前に

フェデレーションの IM and Presence 設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	Microsoft Lync でのスタティック ルートの設定, （2 ページ）	Lync サーバで、Expressway Gateway（チャット + 通話の展開の場合）または IM and Presence サービスのルーティング ノード（チャットのみの展開の場合）のいずれかを指す TLS スタティック ルートを設定します。
ステップ 2	Lync 用の信頼できるアプリケーションの設定, （4 ページ）	Lync サーバで、IM and Presence サービスを信頼できるアプリケーションとして追加し、IM and Presence クラスタ ノードを信頼できるアプリケーション サーバ プールに追加します。
ステップ 3	トポロジのパブリッシュ, （6 ページ）	Lync サーバで、トポロジをコミットします。
ステップ 4	Lync での証明書の設定, （6 ページ）	Lync サーバで証明書をセットアップします。

Microsoft Lync でのスタティック ルートの設定

Lync サーバ上に、次の宛先のいずれかを指す TLS スタティック ルートを作成する必要があります。

- チャット + 通話の展開の場合は、Expressway Gateway へのスタティック ルートを設定します。
- チャット専用の展開の場合は、IM and Presence サービス ルーティング ノードへのスタティック ルートを設定します。

（注） TLS を使用する場合は、スタティック ルートの宛先パターンで使用する FQDN は、Lync のフロント エンド サーバから解決可能である必要があります。FQDN が Expressway Gateway または IM and Presence サービスのルーティング ノードの IP アドレスに解決されることを確認します。

Lync FQDN をパーティション イントラドメイン フェデレーションに使用される IM and Presence サービス ドメインに一致させることはできません。

手順

ステップ 1 Lync Server サーバ管理シェルがインストールされたコンピュータに、ドメイン管理者などのロールでログインします。

ヒント RTCUniversalServerAdmins グループのメンバか、**New-CsStaticRoute** コマンドレットを割り当てたロールベース アクセス コントロール（RBAC）ロールとして、ログインする必要があります。

ステップ 2 [スタート（Start）] > [すべてのプログラム（All Programs）] > [Microsoft Lync Server 2010] > [Lync Server 管理シェル（Lync Server Management Shell）] の順に選択します。

ステップ 3 TLS ルートを定義するには、次のコマンドを入力します。

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination fqdn_of_imp_routing_node -Port
listening_port_imp_routing_node -usedefaultcertificate $true -MatchUri domain_imp
```

引数の説明

パラメータ	説明
-Destination	Expressway Gateway の FQDN（チャット + 通話）または IM and Presence サービス ルーティング ノードの FQDN または IP アドレス（チャット専用）。たとえば、`expGateway.example,com` または `impNode.example.com`。
-Port	Expressway Gateway のリスニング ポート（デフォルト ポートは 65072）または IM and Presence サービスのルーティング ノードのリスニング ポート（デフォルト ポートは 5061）。
-MatchUri	Expressway Gateway ドメイン（チャット + 通話）または lM and Presence サービス（チャット専用）のドメイン。たとえば、`example.com`。

例：

```
$tlsRoute = New-CsStaticRoute -TLSRoute -Destination impNode.example.com -Port 5061
-usedefaultcertificate $true -MatchUri example.com
```

（注）
- ドメインの子ドメインに一致させるには、**-MatchUri** パラメータに、たとえば *.sip.com などのワイルドカード値を指定できます。この値は sip.com サフィックスを持つどのドメインにも一致します。
- Microsoft Lync Server 2013 で IPv6 を使用する場合、**-MatchUri** パラメータの * ワイルドカード オプションはサポートされていません。

ステップ 4 新しく作成されたスタティック ルートを中央管理ストアで保持されていることを確認します。次のコマンドを入力します。

```
Set-CsStaticRoutingConfiguration -Route @{Add=$tlsRoute}
```

（注） IM and Presence サービス ノードをルーティングする場合のみこの手順を実行します。

ステップ 5 新しいスタティック ルートを保持するように設定した場合、コマンドが正常に実行されたことを確認します。次のコマンドを入力します。

```
Get-CsStaticRoutingConfiguration | Select-Object -ExpandProperty Route
```

ステップ 6 Lync のコントロール パネルを開きます。[外部ユーザアクセス（External User Access）] 領域で、次の手順を実行します。

a) [新規（New）] をクリックし、Lync がフェデレーションを実行しているドメイン（IM and Presence サービス ドメイン）のパブリック プロバイダーと VCS Expressway Gateway の FQDN を作成します。

b) 新しいパブリック プロバイダーで、このプロバイダーとのすべての通信を許可するユーザ レベルの検証を設定します。

次の作業

Lync 用の信頼できるアプリケーションの設定, （4 ページ）

Lync 用の信頼できるアプリケーションの設定

Lync サーバで、IM and Presence サービスを信頼できるアプリケーションとして追加し、各 IM and Presence クラスタ ノードを信頼できるアプリケーション サーバ プールに追加します。この手順は、Enterprise Edition と Standard Edition の両方の Lync 展開に適用されます。

手順

ステップ 1 以下のコマンドを使用して、IM and Presence サービス展開に対して信頼できるアプリケーション サーバを作成します。

ヒント プールの登録サービスの FQDN 値を検証するために **Get-CsPool** を入力できます。

```
New-CsTrustedApplicationPool -Identity trusted_application_pool_name_in FQDN_format -Registrar
Lync_Registrar_service_FQDN -Site ID_for_the_trusted_application_pool_site
-TreatAsAuthenticated $true -ThrottleAsServer $true -RequiresReplication $false -OutboundOnly
$false -Computerfqdn first_trusted_application_computer
```

例：

```
New-CsTrustedApplicationPool -Identity trustedpool.sip.com -Registrar lyncserver.synergy.com
-Site 1 -TreatAsAuthenticated $true -ThrottleAsServer $true -RequiresReplication $false
-OutboundOnly $false -Computerfqdn impserverPub.sip.com
```

引数の説明

パラメータ	説明
-Identity	IM and Presence サービス展開の信頼済みアプリケーション プールの名前を入力します。これは FQDN 形式である必要があります。例：`trustedpool.sip.com` **ヒント** Active Directory にはないマシンに関する警告メッセージを無視し、変更を適用します。
-Registrar	プールのレジストラ サービス ID または FQDN。例：`lyncserver.synergy.com` この値は、コマンド Get-CsPool を使用して確認できます。
-Site	信頼できるアプリケーション プールを作成するサイトの数値。 **ヒント** Get-CsSite 管理シェルコマンドを使用します。
-Computerfqdn	IM and Presence サービス ルーティング ノードの FQDN。例：`impserverPub.sip.com` • impserverPub = IM and Presence サービス ホスト名。 • sip.com = IM and Presence サービス ドメイン。

ステップ 2 各IM and Presence サービス ノードに次のコマンドを入力し、新しいアプリケーション プールに信頼できるアプリケーションのコンピュータとしてノードの FQDN を追加します。

New-CsTrustedApplicationComputer -Identity *imp_FQDN* **-Pool** *new_trusted_app_pool_FQDN*

例：

New-CsTrustedApplicationComputer -Identity *impserver2.sip.com* **-Pool** *trustedpool.sip.com*

引数の説明

パラメータ	説明
-Identity	IM and Presence サービス ノードの FQDN。例：`impserver2.sip.com` **（注）** このコマンドを使用して、信頼できるアプリケーションのコンピュータとして IM and Presence サービス ルーティング ノードを追加しないでください。
-Pool	IM and Presence サービス展開で使用される信頼済みアプリケーション プールの FQDN。例：`trustedpool.sip.com`

ステップ 3 新しい信頼済みアプリケーションを作成し、それを新規アプリケーション プールに追加するには、次のコマンドを入力します。

New-CsTrustedApplication -ApplicationID *new_application_name* **-TrustedApplicationPoolFqdn** *new_trusted_app_pool_FQDN* **-Port 5061**

例：

```
New-CsTrustedApplication -ApplicationID imptrustedapp.sip.com -TrustedApplicationPoolFqdn
trustedpool.sip.com -Port 5061
```

引数の説明

パラメータ	説明
-ApplicationID	アプリケーションの名前。これは任意の値にすることができます。例：imptrustedapp.sip.com。
-TrustedApplicationPoolFqdn	IM and Presence サービス展開の信頼済みアプリケーション プール サーバの FQDN。例：`trustedpool.sip.com`
-Port	IM and Presence サービス ノードの SIP リスニング ポート。TLS の場合、ポートは 5061 です。

次の作業

トポロジのパブリッシュ，（6 ページ）

トポロジのパブリッシュ

次の手順は、トポロジをコミットする例を示します。

手順

ステップ 1 Lync サーバ管理シェルにログインします。

ステップ 2 **Enable-CsTopology** コマンドを入力して、トポロジを有効にします。

次の作業

Lync での証明書の設定，（6 ページ）

Lync での証明書の設定

次のタスクを実行して、IM and Presence サービスによるパーティション イントラドメイン フェデレーション用に Lync サーバに証明書をインストールおよび設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Lync への認証局のルート証明書のインストール, （7 ページ）	IM and Presence サービスと Lync 間の TLS 暗号化をサポートするには、Lync 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。
ステップ 2	既存の Lync 署名付き証明書の検証, （10 ページ）	IM and Presence サービスと Lync 間の TLS 暗号化をサポートするには、Lync 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必要です。
ステップ 3	Lync の認証局から署名付き証明書を要求, （11 ページ）	認証局（CA）からの新しい署名付き証明書を要求し、Lync サーバにインストールします。
ステップ 4	CA サーバから証明書をダウンロード, （13 ページ）	CA サーバから新しい署名付き証明書をダウンロードします。
ステップ 5	Lync の署名付き証明書をインポート, （13 ページ）	Lync に新しい署名付き証明書をインポートします。
ステップ 6	Lync への証明書の割り当て, （14 ページ）	Lync サーバで、新しい署名付き証明書を割り当てます。
ステップ 7	Lync サーバでのサービスの再起動, （15 ページ）	Lync フロントエンドサービスを再起動して、構成が有効になるようにします。

Lync への認証局のルート証明書のインストール

TLS の設定は、IM and Presence サービスと Lync との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使用する必要があります。TCP は使用できません。IM and Presence サービスおよび Lync 間の TLS 暗号化をサポートするには、Lync 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、Lync サーバごとにインストールする必要があります。

Lync と IM and Presence サービス サーバで同じ CA を共有することをお勧めします。そうしないと、IM and Presence サービスの証明書に署名した CA のルート証明書も Lync サーバごとにインストールする必要があります。

通常、Lync CA のルート証明書は Lync 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、Lync と IM and Presence サービスが同じ 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 認証局を使用している場合、Microsoft 認証局から Lync 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

別の CA を使用する場合は、次の手順が Lync 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。

（注） 『*Integration Guide for Configuring IM and Presence Service for Interdomain Federation*』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 Lync 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。

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、Lync サーバのハード ディスクに保存します。

手順

ステップ 1 Lync 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 [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）] をクリックしてから、[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。

次の作業

既存の Lync 署名付き証明書の検証, （10 ページ）

関連トピック

統合のトラブルシューティング

既存の Lync 署名付き証明書の検証

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

次のいずれかの OID 値が証明書に割り当てられていることを確認します。

- サーバおよびクライアント認証の両方に証明書が設定されている場合、OID 値は “1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2” です。
- 証明書がサーバ認証のみに設定されている場合、OID 値は “1.3.6.1.5.5.7.3.1” です。

（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 Lync 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 Lync 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

Lync の認証局から署名付き証明書を要求, （11 ページ）

関連トピック

統合のトラブルシューティング

Lync の認証局から署名付き証明書を要求

IM and Presence サービスと Lync との間で TLS 暗号化をサポートするには、Lync の各サーバには、クライアント認証とサーバ認証をサポートする署名付きセキュリティ証明書が必要です。次の手順は、認証局（CA）からの新しい署名付き証明書を要求し、Lync サーバにインストールする方法について説明します。

次の手順は、Windows Server 2003 認証局に基づきます。この手順は、他の Windows サーバのバージョンとは多少異なる場合があります。

（注） CA にはクライアント証明書およびサーバ認証 Extended Key Usage（EKU）をサポートする証明書のテンプレートが必要で、証明書に署名するときにこのテンプレートを使用する必要があります。

Lync サーバに証明書をインストールする前に、次のいずれかの OID 値が証明書に割り当てられていることを確認します。

- サーバおよびクライアント認証の両方に証明書が設定されている場合、OID 値は “1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2” です。
- 証明書がサーバ認証のみに設定されている場合、OID 値は “1.3.6.1.5.5.7.3.1” です。

ヒント 証明書署名要求（CSR）を生成する場合、特定のテンプレート タイプが指定されない場合、デフォルト テンプレート形式が使用されます。ユーザが証明書の登録プロセス中に指定したテンプレートの種類は、証明書で指定されているテンプレートのタイプに一致する必要があります。それ以外の場合は、証明書の登録プロセスが失敗します。

手順

ステップ 1 Lync Server 管理シェルで CSR ファイルを作成するには、次のコマンドを入力します。

```
Request-CsCertificate -New -Type Default -Output filename -ClientEku $true
```

（注） 内部または外部証明書の特定の要求を作成する場合は、**-Type Internal** の代わりに、**-Type External** または **-Type Default** のパラメータを使用します。

証明書に署名するために CA でカスタム証明書テンプレートを使用している場合は、コマンド文字列に **-Template** *template_name* パラメータを追加します。

ステップ 2 Lync サーバにログインし、Web ブラウザを開きます。

ステップ 3 次の URL を開きます。`http://ca_server_IP_address/certsrv`（SSL 暗号化の場合、HTTP ではなく HTTPS を使用）。

ステップ 4 [証明書を要求（Request a certificate）] を選択し、[高度な証明書を要求（Advanced certificate request）] を選択します。

ステップ 5 [Base-64 で暗号化した CMC または PKCS #10 ファイルを使用して証明書要求を提出（Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file）] または [Base-64 で暗号化した PKCS #7 ファイルを使用した更新要求を提出（Submit a renewal request by using a base-64-encoded PKCS #7 file）] を選択します。

ステップ 6 テキスト エディタを使用して作成した要求ファイルを開きます。

ステップ 7 要求ファイルからすべてのテキストをコピーし、ブラウザの [ベース 64 エンコード証明書要求（CMC または PKCS #10 または PKCS #7）（Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7)）] フィールドに貼り付けます。

ステップ 8 [送信（Submit）] をクリックします。

次の作業

CA サーバから証明書をダウンロード, （13 ページ）

CA サーバから証明書をダウンロード

次の手順を実行し、CA サーバからルート証明書をダウンロードします。

手順

ステップ 1 CA サーバにログインします。

ステップ 2 [スタート（Start）] > [管理ツール（Administrative Tools）] > [認証局（Certificate Authority）] を選択し、CA コンソールを起動します。

ステップ 3 [保留中の要求（Pending Requests）] をクリックします。

ステップ 4 右側のペインで送信した証明書の要求を右クリックし、[すべてのタスク（All Tasks）] > [発行（Issue）] を選択します。

ステップ 5 Lync サーバにログインし、Web ブラウザを開きます。

ステップ 6 次の URL を開きます。`http://ca_server_IP_address/certsrv`（SSL 暗号化の場合、HTTP ではなく HTTPS を使用）。

ステップ 7 [保留中の証明書の要求の状態（View the Status of a Pending Certificate Request）] から、証明書の要求をクリックします。

ステップ 8 証明書をダウンロードします。

次の作業

Lync の署名付き証明書をインポート, （13 ページ）

Lync の署名付き証明書をインポート

署名付き証明書をインポートするには、次の手順を実行します。

はじめる前に

（注） 次のいずれかの OID 値が証明書に割り当てられていることを確認します。

- サーバおよびクライアント認証の両方に証明書が設定されている場合、OID 値は “1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2” です。
- 証明書がサーバ認証のみに設定されている場合、OID 値は “1.3.6.1.5.5.7.3.1” です。

手順

Lync Server 管理シェルで次のコマンドを入力し、署名付き証明書をインポートします。

```
Import-CsCertificate -Path "signed_certificate_path" -PrivateKeyExportable $false
```

（注） 証明書に秘密キーが含まれる場合、**-PrivateKeyExportable $true** パラメータを使用します。

次の作業

Lync への証明書の割り当て, （14 ページ）

関連トピック

統合のトラブルシューティング

Lync への証明書の割り当て

次の手順を実行し、証明書を割り当てます。

手順

ステップ 1 [開始（Start）] > [Lync サーバ展開ウィザード（Lync Server Deployment Wizard）] を選択します。

ステップ 2 [Lync サーバ システムのインストールまたはアップデート（Install or Update Lync Server System）] を選択します。

ステップ 3 [もう一度実行（Run Again）] をクリックし、証明書を要求、インストール、または割り当てます。

ステップ 4 [証明書ウィザード（Certificate Wizard）] ウィンドウで、デフォルトの証明書を選択します。

ステップ 5 [割り当て（Assign）] をクリックします。

ステップ 6 証明書の割り当てウィンドウで、[次へ（Next）] をクリックします。

ステップ 7 証明書ストア ウィンドウでインポートされた証明書を選択し、[次へ（Next）] をクリックします。

ステップ 8 証明書の割り当ての概要ウィンドウで [次へ（Next）] をクリックします。

ステップ 9 コマンドの実行ウィンドウで、タスクのステータスに [完了（Completed）] と表示されるまで待機し、[終了（Finish）] を選択します。

ステップ 10 証明書ウィザードのウィンドウを閉じます。

次の作業

Lync サーバでのサービスの再起動, （15 ページ）

Lync サーバでのサービスの再起動

Lync のすべての手順を実行した後、Lync フロント エンド サービスを再起動して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）] > [サービス（Services）] を選択します。

ステップ 2 サービス Lync フロントエンドサーバを右クリックして、[リスタート（Restart）] 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