この統合のための準備

サポートされているドメイン間フェデレーションの統合

このマニュアルでは、IM and Presence サービスと外部ドメイン間にフェデレーテッド ネットワークを設定するための設定手順について説明します。

IM and Presence サービス ノードがフェデレーション可能な、サポートされた外部ドメインは次のとおりです。

- SIP 経由の Microsoft Office 365（企業間）
- SIP 経由の Microsoft Skype for Business 2015（企業間）
- Microsoft Office Communications Server リリース 2007、R2、Microsoft Lync 2010 および 2013（SIP 経由）

（注） IM and Presence サービスは、Microsoft Lync とのドメイン間フェデレーションをサポートします。OCS とのドメイン間フェデレーションへの参照には、別途明示的な指定がない限り、Microsoft Lync が指定されます。

- XMPP 経由の AOL
- XMPP 経由の Cisco WebEx Messenger
- IBM Sametime Server リリース 8.2、8.5（XMPP 経由）

- IM and Presence サービス リリース 9.x 以降（XMPP 経由）

（注） それぞれ IM and Presence サービスが導入されている 2 つのエンタープライズ間にフェデレーションを設定する場合は、XMPP フェデレーションの設定方法について記載されている手順に従ってください。

関連トピック

ハードウェア要件, （2 ページ）
ソフトウェア要件, （3 ページ）

Presence Web Service の API サポート

オープン インターフェイスである Presence Web Service を使用すると、クライアント アプリケーションはユーザ プレゼンス情報を IM and Presence サービスと共有できます。サードパーティ開発者は、このインターフェイスを使用して、ユーザのプレゼンス状態に関する更新を送信および取得するクライアント アプリケーションを構築できます。Presence Web Service の API サポートについて、次の制限事項に注意してください。

- SIP を使用したドメイン間フェデレーションでは、Presence Web Service の API を使用し、シスコ以外のクライアントから多くのプレゼンス情報を取得することができます。ただし、シスコ以外のクライアントの基本的なプレゼンスはサポートされません。
- XMPP を使用したドメイン間フェデレーションでは、Presence Web Service の API を使用してシスコ以外のクライアントからプレゼンス情報を取得することはできません。

Presence Web Service の詳細については、https://developer.cisco.com/site/collaboration/call-control/unified-presence/documentation/index.gspの『*IM and Presence Service Developer Guide*』を参照してください。

ハードウェア要件

シスコ ハードウェア

- IM and Presence サービス ノード。IM and Presence サービス ハードウェア サポートについては、IM and Presence サービス互換性マトリクスを参照してください。
- Cisco Unified Communications Manager のノード。Cisco Unified Communications Manager のハードウェア サポートについては、Cisco Unified Communications Manager の互換性マトリクスを参照してください。
- IM and Presence サービスの企業内の 2 つの DNS サーバ
- Cisco Adaptive Security Appliance（ASA）5500 シリーズ

- SIP フェデレーションの場合のみ、TLS プロキシ機能を実現できる Cisco Adaptive Security Appliance（ASA）の使用を推奨します。XMPP フェデレーションの場合は、いずれのファイアウォールでも十分です。
- Cisco Adaptive Security Appliance（ASA）モデルを選択する場合は、http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_models_home.html にアクセスしてください。TLS プロキシコンポーネントは、すべての 5500 モデルで使用可能です。
- 必ず目的の配置に適したバージョンの Cisco Adaptive Security Appliance（ASA）ソフトウェアを使用してください。ドメイン間フェデレーションを新たに設定する場合は、IM and Presence サービスの互換性マトリクスで、Cisco Adaptive Security Appliance（ASA）ソフトウェアの適切なバージョンを確認してください。

関連トピック

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html
ソフトウェア要件, （3 ページ）

ソフトウェア要件

シスコ ソフトウェア

- IM and Presence Service
- Cisco Unified Communications Manager
- Cisco Adaptive Security Appliance v8.3(1) 以降
- Cisco Adaptive Security Device Manager（ASDM）v6.3 以降
- サポートされている XMPP クライアント：
  - Cisco Unified Personal Communicator リリース 8.5
  - Cisco Jabber for Mac
  - Cisco Jabber for Windows
  - モバイル向け Cisco Jabber IM（Cisco Jabber IM for iPhone、Android、Blackberry）
  - Cisco Jabber for iPad
  - Cisco Jabber for Cius

Microsoft の SIP フェデレーション用ソフトウェア

- Microsoft Skype for Business Server 2015、Standard Edition または Enterprise Edition
- Microsoft Lync 2013 または 2010、Standard Edition または Enterprise Edition
- Microsoft OCS 2007 リリース 2 Server Standard または Enterprise

- Microsoft Office Communicator 2007 リリース 2

AOL の SIP フェデレーション用ソフトウェア

- AOL SIP Access Gateway（SAG）
- AOL Instant Messenger リリース 7.2.6.1 以降

XMPP フェデレーション用ソフトウェア

- Cisco WebEx Messenger
- IBM Sametime Server リリース 8.2

関連項目

ハードウェア要件, （2 ページ）

統合の準備

この統合については、綿密な計画を立てることが重要です。この統合に関する設定を開始する前に、以下の各項目をお読みください。

ルーティング設定

フェデレーテッド ネットワークでのルーティングをどのように設定するかを考えます。まず外部ドメイン宛てのメッセージを、IM and Presence サービス から Cisco Adaptive Security Appliance を経由して外部ドメインにルーティングする方法について考える必要があります。その 1 つの選択肢として、IM and Presence サービスのエンタープライズ導入と Cisco Adaptive Security Appliance との間に、ルーティング エンティティ（ルータ、スイッチ、またはゲートウェイ）を導入するという方法があります。この場合、メッセージはルーティング エンティティから Cisco Adaptive Security Appliance にルーティングされ、さらに Cisco Adaptive Security Appliance から外部ドメインにルーティングされます。

一方、IM and Presence サービスと外部ドメインとの間に Cisco Adaptive Security Appliance をゲートウェイとして導入することもできます。Cisco Adaptive Security Appliance をローカルのエンタープライズ導入内の IM and Presence サービスのゲートウェイとして使用する場合は、Cisco Unified Communications Manager と IM and Presence サービス クライアントが IM and Presence サービス ノードにどのようにアクセスするかを考慮する必要があります。Cisco Unified Communications Manager と IM and Presence サービス クライアントが IM and Presence サービスとは異なるサブネットにある場合、それらは Cisco Adaptive Security Appliance を使用して IM and Presence サービスにアクセスする必要があります。

ネットワーク内の既存のファイアウォールの背後に Cisco Adaptive Security Appliance を導入する場合は、Cisco Adaptive Security Applianceおよび IM and Presence サービスにトラフィックをルーティングする方法について考慮します。既存のファイアウォール上では、IM and Presence サービスの

パブリックアドレスにトラフィックをルーティングするためのルートとアクセスリストを設定します。また、既存のファイアウォールを使用して、外部ドメインへのルートも設定する必要があります。

関連トピック

Cisco Adaptive Security Appliance（ASA）の配置オプション
SIP フェデレーションに関する Cisco Adaptive Security Appliance（ASA）の設定

パブリック IP アドレス

SIP フェデレーションの場合、IM and Presence サービスのパブリック アドレスとして、パブリックにアクセスできるIPアドレスが必要です。割り当てることができるIPアドレスがない場合は、Cisco Adaptive Security Appliance の外部インターフェイスを IM and Presence サービス アドレスのパブリック アドレスとして使用します（Cisco Adaptive Security Appliance を在席情報および IM トラフィック用としてのみ使用している場合）。

Microsoft OCS R2 との SIP フェデレーションでは、複数の IM and Presence サービス ノードを導入する場合でも、必要となるパブリック IP アドレスは 1 つだけです。Cisco Adaptive Security Appliance では、ポート アドレス変換（PAT）を使用して、OCS から適切な IM and Presence サービス ノードへ要求がルーティングされます。

XMPP フェデレーションの場合は、XMPP フェデレーションを有効にした IM and Presence サービス ノードごとにパブリック IP アドレスを公開するか、ただ 1 つのパブリック IP アドレスを公開するかを選択することができます。

- 複数の IP アドレスを公開する場合は、Cisco Adaptive Security Appliance 上で NAT を使用してパブリック アドレスをプライベート アドレスに変換します。たとえば、NAT を使用すると、x.x.x.x:5269 および y.y.y.y:5269 というパブリック アドレスをそれぞれ、a.a.a.a:5269 および b.b.b.b:5269 というプライベート アドレスに変換できます。
- 1 つのパブリック IP アドレスを公開する場合は、Cisco Adaptive Security Appliance 上で PAT を使用して、正しい IM and Presence サービス ノードにマッピングします。たとえば、使用するパブリック IP アドレスが x.x.x.x で、かつ _xmpp-server の DNS SRV レコードが複数あるとします。各レコードのポートはそれぞれ異なりますが、レコードはすべて x.x.x.x に解決されます。そして外部サーバからは、Cisco Adaptive Security Appliance を経由して x.x.x.x:5269、x.x.x.x:15269、x.x.x.x.25269 に要求が送信されるとします。この場合、Cisco Adaptive Security Appliance では、それらの IP アドレスを対象に PAT が実行されます。これにより、それぞれのアドレスは、対応する各 IM and Presence サービス ノードの内部 IP アドレスにマッピングされます。

  たとえば、パブリック IP アドレス x.x.x.x:5269 は a.a.a.a:5269 というプライベート IP アドレス、パブリック IP アドレス x.x.x.x:15269 は b.b.b.b.b:5269 というプライベート IP アドレス、パブリック IP アドレス x.x.x.x:25269 は c.c.c.c:5269 というプライベート IP アドレスにそれぞれマッピングされます。内部的には、すべての IP アドレスが IM and Presence サービス上の同一ポート（5269）にマッピングされます。

関連トピック

外部および内部インターフェイスの設定
DNS の設定，（6 ページ）

パブリック FQDN

SIP フェデレーションの場合、要求メッセージのルーティングは FQDN に基づいて行われます。そのため、ルーティングする IM and Presence サービス ノード（パブリッシャ）の FQDN は、パブリックに解決可能である必要があります。

冗長性およびハイ アベイラビリティ

フェデレーテッド ネットワークに冗長性を確保する方法についても考える必要があります。Cisco Adaptive Security Appliance では、アクティブ/スタンバイ（A/S）導入モデルにより冗長性がサポートされています。

IM and Presence サービスのフェデレーション機能に対してハイ アベイラビリティを実現する必要がある場合は、指定した（フェデレーション）IM and Presence サービス クラスタの手前にロードバランサを導入することができます。

DNS の設定

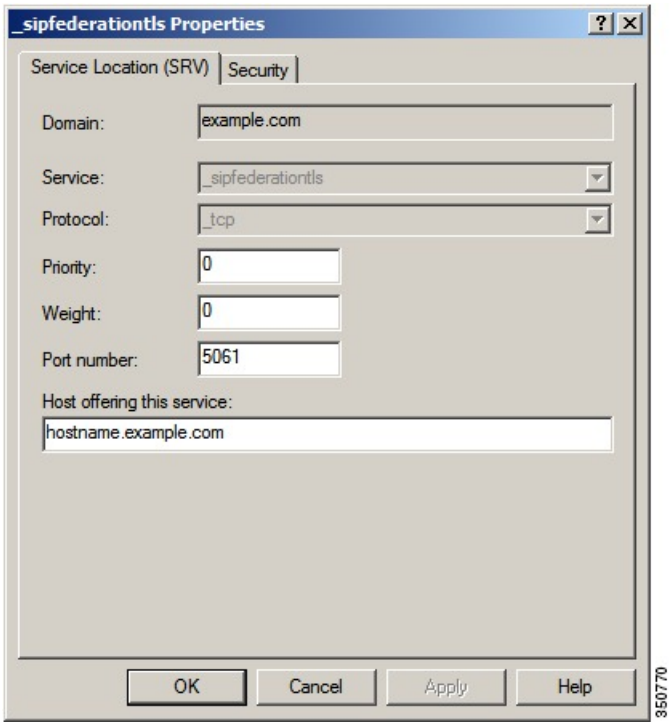
ローカル IM and Presence サービス企業展開では、DNS SRV を通じて他のドメインが IM and Presence サービス ノードを確認できるように、IM and Presence サービスがローカル IM and Presence サービス ドメインに DNS SRV レコードをパブリッシュしなければなりません。DNS SRV レコードは、企業の DMZ 内にある DNS サーバに保管されています。

ローカル IM and Presence サービス展開が複数のドメインを管理している場合は、各ローカル ドメインの DNS SRV レコードを公開します。ユーザが各ローカル ドメインに対して公開する DNS SRV レコードは、同一の FQDN パブリック IP アドレスに解決される必要があります。

Microsoft OCS R2 との SIP フェデレーションの場合は、DNS SRV レコード「_sipfederationtls」をパブリッシュする必要があります。Microsoft 製品のエンタープライズ導入では、IM and Presence サービスを Access Edge サーバ上で Public IM Provider として設定するため、このレコードが必要となります。外部のエンタープライズ導入で IM and Presence サービスから Microsoft ドメインを検出できるようにするためには、その外部ドメインを指す DNS SRV レコードが存在する必要があります。IM and Presence サービス ノードが DNS SRV を使用して Microsoft ドメインを検出できない場合は、IM and Presence サービス上で、その外部ドメインのパブリック インターフェイスに向かうスタティック ルートを設定する必要があります。

DNS SRV レコード「_sipfederationtls_tcp.example.com」の DNS 設定例については、次の図を参照してください。

図 *1*：「*_sipfederationtls*」の *DNS SRV*



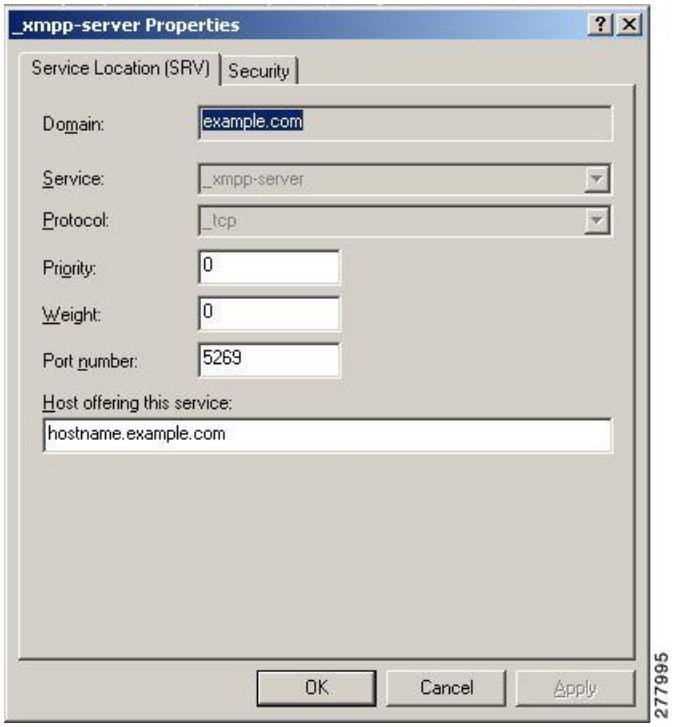
AOL フェデレーションの場合、AOL では「aol.com」ドメインのパブリック DNS サーバで DNS SRV レコード「_sipfederationtls_tcp.aol.com」がパブリッシュされます。このレコードは、AOL SIP Access Gateway に対応する「sip.oscar.aol.com」に解決されます。

DNS SRV レコードはパブリックに解決可能です。そのため、ローカルのエンタープライズ導入内で DNS 転送を有効にしている場合は、DNS クエリーを実行することで、外部のパブリック ドメインに関する情報を取得することができます。DNS クエリーがローカルのエンタープライズ導入内の DNS 情報に全面的に依存している（ローカルのエンタープライズ導入内で DNS 転送を有効にしていない）場合は、外部ドメインを指定する DNS SRV レコード/FQDN/IP アドレスをパブリッシュしなければなりません。スタティック ルートを設定することもできます。

XMPP フェデレーションの場合は、DNS SRV レコード「_xmpp-server」をパブリッシュする必要があります。このレコードにより、フェデレーション XMPP ドメインから IM and Presence サービス ドメインを検出することができるため、両ドメインのユーザは XMPP を介して IM や在席情報をやり取りすることが可能です。同様に外部ドメインでは、IM and Presence サービスから検出できるよう、パブリック DNS サーバで「_xmpp-server」レコードをパブリッシュする必要があります。

DNS SRV レコード "_xmpp-server" の DNS 設定例については、次の図を参照してください。

図 *2*：「*_xmpp-server*」の *DNS SRV*



関連トピック

AOL との SIP フェデレーションのルート SIP 要求

AOL との SIP フェデレーションに使用するデフォルト フェデレーション ルーティング ドメインの変更

認証権限サーバ

SIP フェデレーションの場合、IM and Presence サービスのエンタープライズ導入内の Cisco Adaptive Security Appliance（ASA）と、外部のエンタープライズ導入とは、セキュアな TLS/SSL 接続を介して IM および在席情報を共有します。

各エンタープライズ導入では外部認証局（CA）により署名された証明書を提示する必要があります。ただし、エンタープライズ導入ごとに別々の CA が使用される場合もあります。したがって両者間の相互信頼を実現するためには、それぞれのエンタープライズ導入に他方のエンタープライズ導入の外部 CA からルート証明書をダウンロードする必要があります。

XMPP フェデレーションの場合は、セキュアな TLS 接続を設定するかどうかを選択することができます。TLS を設定する場合は、IM and Presence サービス上で、外部企業の証明書に署名している認証局（CA）のルート証明書をアップロードする必要があります。この証明書は、IM and Presence サービス上の証明書信頼ストア内に存在する必要があります。なぜなら、Cisco Adaptive

Security Appliance では XMPP フェデレーション用の TLS 接続が終端されないためです。Cisco Adaptive Security Appliance は XMPP フェデレーション用のファイアウォールとして機能します。

この統合の前提条件となる設定タスク

統合に関する IM and Presence サービスの設定

（注） ここで説明する前提条件タスクは、SIP フェデレーションと XMPP フェデレーションのどちらにも共通するものです。

手順

ステップ 1 IM and Presence サービスをインストールし、設定します。
ここでは、IM and Presence サービスが正常に動作することを保証するため、以下の確認を行います。

- IM and Presence サービス システム設定トラブルシュータを実行します。
- ローカルな連絡先を IM and Presence サービスに追加できることを確認します。
- クライアントが IM and Presence サービス ノードからアベイラビリティ ステータスを受信していることを確認します。

ステップ 2 IM and Presence サービス ノードと Cisco Unified Communications Manager ノードを『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』の説明のとおりに設定します。IM and Presence サービス ノードが動作しており、問題がないことを確認します。

関連トピック

統合に関する Cisco Adaptive Security Appliance の設定, （10 ページ）

統合に関する Cisco Adaptive Security Appliance の設定

（注）
- SIP フェデレーションには、Cisco Adaptive Security Appliance が必要です。
- XMPP フェデレーションには、ファイアウォールが必要です。基本的なファイアウォール/NAT/PAT 機能を実現するためであれば、Cisco Adaptive Security Appliance を含め任意のファイアウォールを使用することができます。XMPP フェデレーションで TLS プロキシ機能を実現する場合には、Cisco Adaptive Security Appliance は使用しません。

Cisco Adaptive Security Appliance をインストールし、設定します。そのうえで、Cisco Adaptive Security Appliance について次のような基本設定の確認を行います。

手順

ステップ 1 コンソール、HyperTerminal または Web ベースの Adaptive Security Device Manager（ASDM）を介して Cisco Adaptive Security Appliance にアクセスします。

ステップ 2 Cisco Adaptive Security Appliance の適切なライセンスを取得します。Cisco Adaptive Security Appliance の TLS プロキシにはライセンスが必要である点に注意してください。ライセンス情報については、シスコの担当者にお問い合わせください。

ステップ 3 ソフトウェアをアップグレードします（必要な場合）。

ステップ 4 次のコマンドを使用してホスト名を設定します。

```
(config)# hostname name
```

ステップ 5 [デバイス設定（Device Setup）] > [システム時間（System Time）] > [時計（Clock）] を選択するか、CLI から **clock set** コマンドを使用することにより、ASDM で時間帯、日付、および時刻を設定します。次の点に注意してください。

- TLS プロキシを設定する前に、Cisco Adaptive Security Appliance 5500 で時計を設定します。
- Cisco Adaptive Security Appliance では IM and Presence サービス クラスタと同じ NTP サーバを使用することが推奨されます。Cisco Adaptive Security Appliance と IM and Presence サービス ノードとの間で時計が同期されていない場合は、証明書の有効性が確認できないために TLS 接続が正常に確立されないことがあります。
- NTP サーバ アドレスを表示するには、**ntp server** *server_address* コマンドと **show ntp associat | status** コマンドを使用して、NTP サーバのステータスを表示します。

ステップ 6 Cisco Adaptive Security Appliance 5500 のモードを確認します。Cisco Adaptive Security Appliance 5500 は、デフォルトでシングルモードおよびルーテッドモードが使用されるよう設定されています。

- 現在のモードを確認します。この値は、デフォルトでシングル モードとなります。

```
(config)# show mode
```

- 現在のファイアウォール モードを確認します。この値は、デフォルトでルーテッド モードとなります。

```
(config)# show firewall
```

- 外部インターフェイスおよび内部インターフェイスを設定します。
- 基本 IP ルートを設定します。

関連トピック

外部および内部インターフェイスの設定
スタティック IP ルートの設定
統合に関する IM and Presence サービスの設定, （9 ページ）