SIP フェデレーション統合のトラブルシューティング

このセクションでは、SIP フェデレーション統合のトラブルシューティング方法について説明します。

Cisco 適応型セキュリティ アプライアンスの一般的な問題と推奨されるアクション

ここでは、Cisco 適応型セキュリティアプライアンスの一般的な問題と推奨されるアクションについて説明します。

証明書構成の問題

IM および Presence サービスと Cisco 適応型セキュリティ アプライアンス間の証明書の障害

IM and Presence Service と Cisco 適応型セキュリティ アプライアンス 間の証明書構成が失敗しています。

Cisco 適応型セキュリティ アプライアンス の時刻とタイムゾーンが正しく構成されていない可能性があります。

- Cisco 適応型セキュリティアプライアンスの時刻とタイムゾーンを設定します。
- IM and Presence Service と Cisco Unified Communications Managerで時刻とタイムゾーンが正しく構成されていることを確認します。

この統合の事前前提構成タスク

Cisco 適応型セキュリティアプライアンスと Microsoft Access Edge 間の証明書の障害

Cisco 適応型セキュリティアプライアンス と Microsoft Access Edge 間の証明書構成は、Cisco 適応型セキュリティ アプライアンスでの証明書の登録時に失敗します。

Cisco 適応型セキュリティアプライアンスで SCEP 登録を使用している場合、SCEP アドオンが正しくインストールおよび構成されていない可能性があります。SCEP アドオンをインストールして設定します。

関連情報

CA トラストポイント

SSL ハンドシェイクの証明書エラー

SSL ハンドシェイクに証明書エラーが表示されます。

証明書に FQDN がありません。IM and Presence Service CLI でドメインを設定し、IM and Presence Service で証明書を再生成して FQDN を設定する必要があります。証明書を再生成する場合は、IM and Presence Service で SIP プロキシを再起動する必要があります。

VeriSign に証明書署名要求を送信する際のエラー

証明書の登録に VeriSign を使用しています。証明書署名要求を VeriSign Web サイトに貼り付けると、エラー（通常は 9406 または 9442 エラー）が表示されます。

証明書署名要求のサブジェクト名に情報がありません。更新証明書署名要求（CSR）ファイルを VeriSign に送信する場合は、証明書署名要求のサブジェクト名に次の情報を含める必要があります。

- 国（2 文字の国コードのみ）
- 州（略語なし）
- 地域（略語なし）
- 組織名
- 組織単位
- 共通名（FQDN）

subject-name 行エントリの形式は次のとおりです。

```
(config-ca-trustpoint)# subject-name cn=fqdn、U=organizational_unit_name、C=country、St=state、L=locality、O=organization
```

関連トピック

VeriSign の新しいトラストポイントの生成

IM および Presence Service のドメインまたはホスト名が変更された場合の SSL エラー

CLI から IM and Presence Service ドメインを変更すると、 IM and Presence Service と Cisco 適応型セキュリティアプライアンスの間で SSL 証明書エラーが発生します。

CLI から IM and Presence Service のドメイン名を変更すると、 IM and Presence Service の自己署名証明書 sipproxy.pem が再生成されます。そのため、sipproxy.pem 証明書を Cisco Cisco 適応型セキュリティアプライアンスに再インポートする必要があります。具体的には、Cisco Cisco 適応型セキュリティアプライアンスの現在の sipproxy.pem 証明書を削除し、（再生成された）Cisco 適応型セキュリティアプライアンス の sipproxy.pem 証明書を再インポートする必要があります。

TLS プロキシ クラス マップ作成時のエラー

TLS プロキシ クラス マップを設定すると、次のエラーが表示されます。

```
ciscoasa(config)# class-map ent_imp_to_external

ciscoasa(config-cmap)# match access-list ent_imp_to_external

エラー：指定された ACL（ent_imp_to_external）が存在しないか、そのタイプが match コマンドでサポートされていません。

ciscoasa(config-cmap)# exit

ciscoasa(config)# class-map ent_external_to_imp

ciscoasa(config-cmap)# match access-list ent_external_to_imp

エラー: 指定された ACL（ent_external_to_imp）が存在しないか、そのタイプが match コマンドでサポートされていません。

ciscoasa(config-cmap)#
```

外部ドメインのアクセスリストが存在しません。上記の例では、ent_external_to_imp というアクセス リストは存在しません。**access list** を使用して、外部ドメインの拡張アクセス リストを作成します。

関連情報 -

アクセス リストの構成要件

TLS プロキシ デバッグ コマンド

サブスクリプションが Access Edge に到達しない

Microsoft Office Communicator からのサブスクリプションが Access Edge に到達しない。OCS は、Access Edge をピアとして使用するネットワーク機能エラーを報告します。Access Edge サービスが開始されません。

Access Edge では、[許可（Allow）] タブと [IM プロバイダー（IM provider）] タブの両方で IM and Presence Service ドメインを構成できます。IM and Presence Service ドメインは、[IM プロバイダー（IM Provider）] タブでのみ構成する必要があります。Access Edge で、[許可（Allow）]

タブから IM and Presence Service ドメイン エントリを削除します。[IM プロバイダー（IM Provider）] タブに IM and Presence Service ドメインのエントリがあることを確認します。

（注） IM and Presence Service は複数のドメインをサポートします。各 IM and Presence ドメインを確認して、[許可（Allow）] タブに削除する必要がある誤ったエントリがあるかどうかを確認してください。

アップグレード後の Cisco 適応型セキュリティ アプライアンスの問題

Cisco 適応型セキュリティ アプライアンスは、ソフトウェアのアップグレード後に起動しません。

TFTP サーバを使用し、Cisco 適応型セキュリティ アプライアンスの ROM モニタ（ROMMON）を使用して、新しいソフトウェア イメージを Cisco 適応型セキュリティ アプライアンスにダウンロードできます。ROMMON は、TFTP および関連する診断ユーティリティを介したイメージのロードと取得に使用されるコマンドライン インターフェイスです。

ステップ 1 コンソール ケーブル（Cisco 適応型セキュリティ アプライアンス に付属している青色のケーブル）をコンソール ポートから近くの TFTP サーバのポートに接続します。

ステップ 2 ハイパーターミナルまたは同等のものを開きます。

ステップ 3 プロンプトが表示されたら、すべてのデフォルト値を受け入れます。

ステップ 4 Cisco 適応型セキュリティ アプライアンスを再起動します。

ステップ 5 ブートアップ中に ESC を押して ROMMON にアクセスします。

ステップ 6 次の一連のコマンドを入力して、Cisco 適応型セキュリティ アプライアンス が TFTP サーバからイメージをダウンロードできるようにします。

```
ip asa_inside_interface server tftp_server interface ethernet 0/1 file name_of_new_image
```

（注） 指定するイーサネット インターフェイスは、Cisco 適応型セキュリティ アプライアンス の内部インターフェイスと同等である必要があります。

ステップ 7 TFTP サーバ上の推奨される場所（TFTP ソフトウェアによって異なる）にソフトウェア イメージを配置します。

ステップ 8 次のコマンドを入力して、ダウンロードを開始します。

```
tftp dnld
```

（注） TFTP サーバが別のサブネットにある場合は、ゲートウェイを定義する必要があります。

Microsoft OCS 2008 に署名付き Microsoft CA サーバ クライアント認証証明書をインストールできない

Microsoft CA によって署名されたサーバ クライアント認証証明書を、Windows 2008 を実行している Microsoft Office Communications Server（OCS）のローカル コンピュータ ストアにインストールすることはできません。現在のユーザー ストアからローカル コンピュータ ストアに証明書をコピーしようとすると、秘密キーが見つからないというエラー メッセージが表示されて失敗します。

以下の手順を実行できます。

1. ローカル ユーザーとして OCS にログインします。
2. 証明書を作成します。
3. CA サーバーからの証明書を承認します。
4. OCS にログオンしている間に、証明書をファイルにエクスポートし、秘密キーがエクスポートされていることを確認します。
5. OCS（ローカル コンピュータ）からログオフします。
6. OCS に再度ログインしますが、今回は OCS ドメイン ユーザーとしてログインします。
7. 証明書ウィザードを使用して、証明書ファイルをインポートします。証明書がローカル コンピュータ ストアにインストールされます。[OCS 証明書（OCS certificate）] タブで証明書を選択できるようになりました。

統合に関する一般的な問題と推奨されるアクション

ここでは、統合に関する一般的な問題と推奨されるアクションについて説明します。

可用性交換を取得できません

問題　Cisco Jabber と Microsoft Office Communicator の間で可用性情報を交換できません。

解決法　OCS/アクセスエッジ、 IM and Presence Service 、および Cisco Jabber について記載されているトラブルシューティング手順を実行します。

OCS/Access Edge：

1. Access Edge のパブリック インターフェイスで証明書が正しく設定されていない可能性があります。Microsoft CA を使用している場合は、OID 値 1.3.6.1.5.5.7.3.1、1.3.6.1.5.5.7.3.2 を使用していることを確認します。証明書の [全般（General）] タブに誤った値が表示されます（正しい場合は表示されません）。また、 IM and Presence Service と Access Edge 間の TLS ハンドシェイクの ethereal トレースに誤った値が表示されることもあります。

証明書タイプが「その他」で、OID 値が 1.3.6.1.5.5.7.3.1、1.3.6.1.5.5.7.3.2 の Access Edge のパブリック インターフェイスの証明書を再生成します。

2. フロントエンド サーバーがOCSで実行されていない可能性があります。

   「Office Communications Server Front-End」サービスが実行されていることを確認します。このサービスを確認するには、**[スタート（Start）]**>**[プログラム（Administrative）]**>**[管理ツール（Administrative Tools）]**>**[コンピュータの管理（Computer Management）]**の順に選択します。**[サービスとアプリケーション（Services and Applications）]** で、**[サービス（Services）]** を選択し、「Office Communications Server Front-End」 サービスを見つけます。実行中の場合、このサービスのステータスは「開始」になります。

IM and Presence Service

1. IM and Presence Serviceで証明書が正しく設定されていない可能性があります

   IM and Presence Serviceの正しい sipproxy-trust 証明書を生成します。

2. スタティック ルートを使用している場合は、Access Edge のパブリック インターフェイスを指すスタティック ルートを設定します。スタティック ルートでは、ルート タイプを「domain」に設定し、逆の接続先パターンを設定する必要があります。たとえば、フェデレーション ドメインが abc.com の場合、接続先アドレスパターンは 「.com.abc.*」に設定する必要があります。スタティック ルートは、[Cisco Unified CM IM and Presence Administration] を使用して、**[プレゼンス（Presence）]** > **[ルーティング（Routing）]** > **[スタティック ルート（Static Routes）]** を選択して設定します。

3. DNS SRV のチェックを実行し、両側が影響を受けるユーザーのドメインを解決できることを確認します。

Cisco Jabber クライアント：

Cisco Jabber は、クライアント コンピュータから誤った DNS 設定を取得する可能性があります。次の手順を実行する必要があります。

1. クライアント コンピュータの DNS 構成を確認します。
2. DNS 設定を変更した場合は、Cisco Jabberを再起動します。

関連トピック

外部 Access Edge インターフェイスの証明書構成
IM および Presence サービスの新規証明書の生成
SIP フェデレーションの DNS 構成

IM の送受信の問題

Microsoft Office Communicator ユーザーと Cisco Jabber 8.0 ユーザー間の IM の送受信に問題があります。

DNS 設定、Access Edge、Microsoft Office Communicator クライアント、および IM and Presence Serviceについてリストされているトラブルシューティング手順を実行します。

DNS の設定：

DNS SRV レコードが作成されていないか、正しく設定されていない可能性があります。DNS SRV レコードがすべてのドメインに対して正しく設定されているかどうかを確認します。IM and Presence Service と Access Edge の両方から type=srv の nslookup を実行します。

Access Edge で

1. Access Edge のコマンドプロンプトから、 **`nslookup`**と入力します。
2. **`set type=srv`** と入力します。
3. IM and Presence ドメインの SRV レコードを入力します。例：**_sipfederationtls._tcp.abc.com** ここで、**abc.com** はドメイン名です。SRV レコードが存在する場合は、 IM and Presence Service/Cisco 適応型セキュリティ アプライアンス の FQDN が返されます。

   IM and Presence Service で：

4. リモート アクセス アカウントを使用して、 IM and Presence Service ノードに ssh 接続します。
5. 上記の Access Edge と同じ手順を実行しますが、この場合は OCS ドメイン名を使用します。

Microsoft Office Communicator クライアント：

Microsoft Office Communicator 2007 ユーザーのプレゼンスが [応答不可（DND）] に設定されている場合があります。Microsoft Office Communicator 2007 が DND に設定されている場合、 は他のユーザーからの IM を受信しません。Microsoft Office Communicator ユーザーのプレゼンスを別の状態に設定します。

IM and Presence Service

1. DNS SRV の代わりにスタティック ルートを使用している場合は、スタティック ルートが正しく構成されていない可能性があります。Access Edge のパブリック インターフェイスを指すスタティック ルートを構成します。スタティック ルートでは、ルート タイプを「domain」に設定し、逆の接続先パターンを設定する必要があります。たとえば、フェデレーション ドメインが 「abc.com」 の場合、宛先アドレス パターンは 「.com.abc.*」に設定する必要があります。**Cisco Unified CM IM and Presence 管理**で、**[プレゼンス（Presence）] > [ルーティング（Routing）] > [スタティック ルート（Static Routes）]**を選択することで、スタティック ルートが構成されます。
2. フェデレーション IM コントローラ モジュールのステータスが無効になっている可能性があります。**[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）]**で**[システム（System）] > [サービス パラメータ（Service Parameters）]** を選択し、[SIP プロキシ（SIP Proxy）] サービスを選択します。ウィンドウの下部で、**[IM ゲートウェイ ステータス（IM Gateway Status）]** パラメータが [オン（On）] に設定されていることを確認します。
3. フェデレーション ドメインが追加されていないか、正しく設定されていない可能性があります。**Cisco Unified CM IM and Presence Administration** で、**[プレゼンス（Presence）] >**

[ドメイン間フェデレーション（Inter-Domain Federation）] を選択し、正しいフェデレーション ドメインが追加されていることを確認します。

関連情報 -

SIP フェデレーションの DNS 構成

SIP フェデレーション ドメインの追加

短期間で可用性と IM 交換が失われる

ユーザーは Cisco Jabber と Microsoft Office Communicator の間で可用性と IM を共有できますが、しばらくすると互いの可用性が失われ、IM を交換できなくなります。

OCS/Access Edge：

1. Access Edge では、内部エッジと外部エッジの両方に同じ FQDN が設定されている場合があります。また、DNS には、その FQDN に 2 つの「A」レコードエントリが存在する場合があります。1 つは外部エッジの IP アドレスに解決し、もう 1 つは内部エッジの IP アドレスに解決します。

   Access Edge で、内部エッジの FQDN を変更し、更新されたレコードエントリを DNS に追加します。Access Edge の内部 IP に最初に解決された DNS エントリを削除します。また、Access Edge の内部エッジの証明書を再設定します。

2. OCS のグローバル設定とフロントエンドのプロパティで、Access Edge の FQDN が誤って入力されている可能性があります。OCS で、内部エッジの新しい FQDN を反映するようにサーバーを再設定します。

DNSの設定：

DNS SRV レコードが作成されていないか、正しく設定されていない可能性があります。必要な「A」レコードと SRV レコードを追加します。

関連情報 -

SIP フェデレーションの外部サーバー コンポーネントの構成

可用性状態の変更と IM 配信時間の遅延

Cisco Jabber と Microsoft Office Communicator の間で IM and Presence Service の状態変更の配信時間に遅延があります。

IM and Presence Service ノードでは、Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context に対して **[空の TLS フラグメントを無効にする（Disable Empty TLS Fragments）]** オプションが選択されていない場合があります。

ステップ 1 **Cisco Unified CM IM and Presence Administration** のユーザ インターフェイスにログインします。**[システム（System）] > [システム（System）] > [TLS コンテキスト設定（TLS Context Configuration）]** を選択します。

ステップ 2 **[Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context]** をクリックします。

ステップ 3 [TLS コンテキスト情報（TLS Context Information）] エリアで、**[空の TLS フラグメントを無効にする（Disable Empty TLS Fragments）]** チェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

可用性サブスクリプションの試行後に 403 FORBIDDEN が返される

IM and Presence Service は、Microsoft Office Communicator ユーザの可用性に登録しようとし、OCS サーバーから 403 FORBIDDEN メッセージを受信します。

Access Edge サーバーで、 IM and Presence Service ノードが IM サービス プロバイダ リストに追加されていない可能性があります。Access Edge サーバーで、 IM and Presence Service ノードのエントリを IM サービス プロバイダー リストに追加します。Access Edge の DNS サーバで、IM and Presence Service ノードのパブリック アドレスを指す IM and Presence Service ドメインの _sipfederationtls レコードがあることを確認します。

または

Access Edge サーバーで、 IM and Presence Service ノードが許可リストに追加されている可能性があります。Access Edge サーバーで、 IM and Presence Service ノードを指すすべてのエントリを許可リストから削除します。

関連情報 -

SIP フェデレーションの外部サーバー コンポーネントの構成

NOTIFY メッセージのタイムアウト

TCP を使用して IM and Presence Service と Microsoft OCS の間で直接フェデレーションを行う場合、NOTIFY メッセージの送信時に IM and Presence Service がタイムアウトします。

IM and Presence Service ノードでは、**[Record-Route ヘッダーでトランスポートを使用（ Use Transport in Record-Route Header）]** を有効にする必要がある場合があります。

ステップ 1 **Cisco Unified CM IM and Presence Administration** のユーザーインターフェイスにログインします。**[システム（System）] > [サービスパラメータ（Service Parameters）]** を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン リストからノードを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストから、**[Cisco SIP プロキシ（Cisco SIP Proxy）]** サービスを選択します。

ステップ 4 [SIP パラメータ（クラスタ全体）（SIP Parameters (Clusterwide)）] セクションで、[Record-Route ヘッダーでトランスポートを使用（Use Transport in Record-Route Header）] パラメータで **[オン（ On ）]** を選択します。

ステップ 5 [**保存（Save**）] をクリックします。

IM および Presence サービスの証明書は承認されません

Access Edge が IM and Presence Serviceからの証明書を受け入れていません。

IM and Presence Service/Cisco 適応型セキュリティアプライアンス と Access Edge 間の TLS ハンドシェイクが失敗している可能性があります。

OCS/Access Edge：

1. Access Edge の IM プロバイダー リストに IM and Presence Service ノードのパブリック FQDN が含まれており、 IM and Presence Service 証明書のサブジェクト CN と一致していることを確認します。許可リストに IM and Presence Serviceの FQDN を入力しないことを選択した場合は、 IM and Presence Service 証明書のサブジェクト CN が IM and Presence Service ドメインの SRV レコードの FQDN に解決されることを確認する必要があります。 。
2. Access Edge で FIPS が有効になっていることを確認します（TLSv1 を使用）。
3. フェデレーションが OCS でグローバルに有効になっており、フロント エンド サーバーで有効になっていることを確認します。
4. DNS SRV の解決に失敗した場合は、DNS が正しく設定されていることを確認し、Access Edge から type=srv の nslookup を実行します。
5. Access Edge のコマンドプロンプトから、 **`nslookup`**と入力します。
6. **`set type=srv`** と入力します。
7. たとえば、 IM and Presence Service ドメインの SRV レコードを入力します。 **_sipfederationtls._tcp.abc.com** ここで、 **abc.com** はドメイン名です。SRV レコードが存在する場合は、 IM and Presence Service/Cisco 適応型セキュリティ アプライアンス の FQDN が返されます。

IM and Presence サービス/Cisco 適応型セキュリティアプライアンス：

IM and Presence サービス と Cisco 適応型セキュリティアプライアンスの暗号を確認します。**IM and Presence Service Administration** にログインし、**[システム（System）]** > **[セキュリティ（Security）]** > **[TLS コンテンツ構成（TLS Context Configuration）]** > **[デフォルト Cisco SIP プロキシ ピア認証 TLS コンテンツ（Default Cisco SIP Proxy Peer Auth TLS Context）]**を選択し、「TLS_RSA_WITH 3DES_EDE_CBC_SHA」暗号が選択されていることを確認します。

OCS でのフロントエンド サーバの起動に関する問題

OCS のフロントエンド サーバーが起動しない。

OCS では、Access Edge のプライベート インターフェイスの FQDN が承認済みホストのリストで定義されている可能性があります。OCS の承認済みホストのリストから Access Edge のプライベート インターフェイスを削除します。

OCS のインストール中に、RTCService と RTCComponentService という 2 つの Active Directory ユーザー アカウントが作成されます。これらのアカウントには管理者が定義したパスワードが与えられますが、これらのアカウントの両方で [パスワードを無期限にする（Password never expires）] オプションはデフォルトで選択されていないため、パスワードは定期的に期限切れになります。OCS サーバーの RTCService または RTCComponentService のパスワードをリセットするには、次の手順に従います。

ステップ 1 ユーザー アカウントを右クリックします。
ステップ 2 **[パスワードのリセット（Reset Password）]** を選択します。
ステップ 3 ユーザー アカウントを右クリックします。
ステップ 4 [プロパティ（Properties）] を選択します。
ステップ 5 **[アカウント（Accounts）]** タブを選択します。
ステップ 6 [パスワードを無期限にする（Password Never Expires）] チェックボックスをオンにします。
ステップ 7 **[OK]** をクリックします。

リモートデスクトップから Edge にアクセスできない

Windows XP で FIPS が有効になっている Access Edge Server に正常にリモート デスクトップを接続できません。

これは、既知の Microsoft 問題です。この問題を解決するための回避策には、Windows XP コンピュータにリモートデスクトップ接続アプリケーションをインストールする必要があります。リモート デスクトップ接続 6.0 をインストールするには、次の Microsoft URL の手順に従ってください。

http://support.microsoft.com/kb/811770

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。