SIPフェデレーション統合に関するトラブルシューティング

一般的な Cisco Adaptive Security Appliance の問題と推奨される操作

証明書の設定に関する問題

IM and Presence サービスと Cisco Adaptive Security Appliance の間での証明書失敗

IM and Presence サービス と Cisco Adaptive Security Appliance 間の証明書の設定にエラーがあります。

Cisco Adaptive Security Appliance の時刻とタイム ゾーンが正しく設定されていない可能性があります。

- Cisco Adaptive Security Appliance で時刻とタイム ゾーンを設定します。
- IM and Presence サービス と Cisco Unified Communications Manager で時刻とタイム ゾーンが正しく設定されていることを確認します。

この統合の前提条件となる設定タスク

Cisco Adaptive Security Appliance と Microsoft Access Edge 間の証明書に関するエラー

Cisco Adaptive Security Appliance への証明書の登録時に、Cisco Adaptive Security Appliance と Microsoft Access Edge 間の証明書の設定が失敗しました。

Cisco Adaptive Security Appliance で SCEP の登録を使用している場合、SCEP アドオンのインストールと設定が正しく行わ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。

関連トピック

CA トラストポイント

SSL ハンドシェイクでの証明書に関するエラー

SSL ハンドシェイクで証明書のエラーが表示されます。

証明書に FQDN がありません。IM and Presence サービス CLI でドメインを設定し、IM and Presence サービスで FQDN がある証明書を再生成する必要があります。証明書を再生成する場合、IM and Presence サービスで SIP プロキシを再起動する必要があります。

関連トピック

CLI から IM and Presence サービス ドメインを設定します。

証明書署名要求を VeriSign に送信するときにエラーが発生する

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 の 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。

証明書署名要求の件名に情報が足りません。更新の証明書署名要求（CSR）ファイルを VeriSign に送信する場合、証明書署名要求の件名には次の情報を含める必要があります。

- 国（Country）（2 文字の国コードのみ）
- 都道府県（State）（省略なし）
- 市区町村（Locality）（省略なし）
- 組織名（Organization Name）
- 組織
- 一般名（Common Name）（FQDN）

件名行エントリは次の形式にする必要があります。

```
(config-ca-trustpoint)# subject-name
cn=fqdn,U=organisational_unit_name,C=country,St=state,L=locality,O=organisation
```

関連トピック

VeriSign 用の新しいトラストポイントの生成

IM and Presence サービスのドメインまたはホスト名を変更する際の SSL エラー

CLI から IM and Presence サービス ドメインを変更すると、IM and Presence サービス と Cisco Adaptive Security Appliance 間で SSL 証明書のエラーが発生します。

CLI から IM and Presence サービス ドメイン名を変更する場合、IM and Presence サービスの自己署名証明書 sipproxy.pem が再生成されます。そのため、sipproxy.pem 証明書を Cisco Adaptive Security Appliance に再インポートする必要があります。具体的には、Cisco Adaptive Security Appliance の現在の sipproxy.pem 証明書を削除し、（再生成された）sipproxy.pem 証明書を再インポートします。

関連トピック

IM and Presence サービスと Cisco Adaptive Security Appliance の間でのセキュリティ証明書交換

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きに、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
ERROR: Specified ACL (ent_imp_to_external) either does not exist or its type is not supported
by the match command.
ciscoasa(config-cmap)# exit
ciscoasa(config)# class-map ent_external_to_imp
ciscoasa(config-cmap)# match access-list ent_external_to_imp
ERROR: Specified ACL (ent_external_to_imp) either does not exist or its type is not supported
by the match command.
ciscoasa(config-cmap)#
```

外部ドメインのアクセス リストが存在しません。前述の例では、ent_foreign_to_cup というアクセス リストが存在しません。**access list** コマンドを使用して、外部ドメインの拡張アクセス リストを作成してください。

関連トピック

アクセス リストの設定の要件
TLS プロキシのデバッグ 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 に到達しません。OCS から、ピアとしての Access Edge に関するネットワーク機能エラーがレポートされます。Access Edge サービスが起動しません。

Access Edge では、[許可（Allow）] タブと [IM プロバイダ（IM Provider）] タブの両方で IM and Presence サービス ドメインを設定できます。IM and Presence サービス ドメインは、[IM プロバイダ（IM Provider）] タブでのみ設定します。Access Edge の [許可（Allow）] タブから IM and Presence サービス ドメインを削除します。[IM Provider（IM プロバイダ）] タブに IM and Presence サービス ドメインのエントリがあることを確認します。

（注） IM and Presence サービスは複数のドメインをサポートします。各 IM and Presence ドメインを必ず確認し、[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ます。

アップグレード後の Cisco Adaptive Security Appliance の問題

ソフトウェアのアップグレード後に Cisco Adaptive Security Appliance がブートしません。

新しいソフトウェア イメージは、TFTP サーバおよび Cisco Adaptive Security Appliance の ROM Monitor（ROMMON）を使用して Cisco Adaptive Security Appliance にダウンロードできます。ROMMON は、TFTP や関連する診断ユーティリティでイメージのロードと取得を行うために使用できるコマンドライン インターフェイスです。

手順

ステップ 1 コンソール ポートから近くの TFTP サーバのポートにコンソール ケーブル（Cisco Adaptive Security Appliance に付属する青色のケーブル）を接続します。

ステップ 2 HyperTerminal または同等のものを開きます。

ステップ 3 表示されるすべてのデフォルト値を受け入れます。

ステップ 4 Cisco Adaptive Security Appliance をリブートします。

ステップ 5 ブート時に 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 Adaptive Security Appliance をイネーブルにし、TFTP サーバからイメージをダウンロードします。

```
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 Adaptive Security Appliance の Inside インターフェイスと一致する必要があります。

ステップ 7 TFTP サーバのソフトウェア イメージを推奨される場所（TFTP ソフトウェアによって異なります）に保存します。

ステップ 8 ダウンロードを開始するには、次のコマンドを入力します。

```
tftp dnld
```

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

署名付き Microsoft CA サーバ-クライアント認証証明書を Microsoft OCS 2008 で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は、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できません。現在のユーザ ストアからローカルのコンピュータ ストアへ証明書をコピーしようとすると、秘密キーがないというエラー メッセージで失敗します。

次の手順を実行できます。

1. ローカル ユーザとして OCS にログインします。
2. 証明書を作成します。
3. CA サーバから証明書を承認します。
4. OCS にログイン中に、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、この場合は OCS ドメイン ユーザとしてログインします。
7. 証明書ファイルをインポートするのに証明書ウィザードを使用します。証明書は、ローカル コンピュータ ストアにインストールされます。この時点で、[OCS 証明書（OCS Certificate）] タブで証明書を選択できるようになります。

一般的な Cisco Adaptive Security Appliance の問題と推奨される操作

アベイラビリティを交換できない

問題 Cisco Jabber と Microsoft Office Communicator 間でアベイラビリティ情報を交換できません。

解決法 OCS/Access Edge、IM and Presence サービス、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、1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2 という OID 値を使用していることを確認します。証明書の [全般（General）] タブには正しくない値が表示されます（正しい場合は表示されません）。また、IM and Presence サービスと Access Edge 間の TLS ハンドシェイクの Ethereal トレースでも正しくない値を確認できます。

証明書の種類が [その他（Other）] 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（Programs）] > [管理ツール（Administrative Tools）] > [コンピュータの管理（Computer Management）] を選択します。[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] サービスを確認します。実行されている場合、このサービスのステータスは [開始（Started）] です。

IM and Presence サービス：

1 IM and Presence サービ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。

IM and Presence サービスの正しい 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、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 ルートは「ドメイン」に設定されたルート タイプを持ち、反転した宛先パターンが設定されている必要があります。たとえば、フェデレーション ドメインが “abc.com” である場合は、宛先アドレスのパターンは .com .abc.* に設定する必要があります。スタティック ルートを設定するには、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）] を選択します。

3 DNS SRV のチェックが実行され、両側が影響を受けるユーザ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 コンピュータから不正な DNS 設定を取得する可能性があります。以下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 設定を確認します。
2 DNS 設定を変更する場合は、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の設定
IM and Presence サービスでの新しい証明書の生成
SIP フェデレーションの DNS 設定

IM の送受信に関する問題

Microsoft Office Communicator ユーザと Cisco Jabber 8.0 ユーザ間で IM を送受信するときに問題があります。

DNS 設定、Access Edge、Microsoft Office Communicator クライアント、IM and Presence サービスについて記載されているトラブルシューティングを実行します。

DNS 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 と Access Edge の両方からの type=srv に対して nslookup を実行します。

Access Edge 側：

1. Access Edge のコマンド プロンプトに 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。たとえば、**_sipfederationtls._tcp.abc.com** と入力します（この **abc.com** はドメイン名です）。SRV レコードが存在する場合、IM and Presence サービスまたは Cisco Adaptive Security Appliance の FQDN が返されます。
   IM and Presence サービス：
4. リモート アクセス アカウントを使用し、ssh で IM and Presence サービス ノードにログインします。
5. 前述の Access Edge と同様の手順を実行します。ただし、ここでは 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 ユーザは、自分のプレゼンスを [取り込み中（Do Not Disturb）]（DND）に設定している可能性があります。Microsoft Office Communicator 2007 が DND に設定されている場合、他のユーザから IM を受信しません。Microsoft Office Communicator ユーザのプレゼンスを別の状態に設定します。

IM and Presence サービス：

1. DNS SRV ではなくスタティック ルートを使用している場合、スタティック ルートが正しく設定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 ルートを設定します。スタティック ルートは「ドメイン」に設定されたルート タイプを持ち、反転した宛先パターンが設定されている必要があります。たとえば、フェデレーション ドメインが “abc.com” である場合は、宛先アドレスのパターンは “.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** 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）] を選択して設定します。
2. [フェデレーション IM コントロール モジュールのステータス（Federation IM Control Module Status）] がディセーブルにされている可能性があります。**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 サービス（SIP Proxy service）] 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 パラメータが設定されていることを確認します。
3. フェデレーテッド 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、正しいフェデレーテッド ドメインが追加されていることを確認します。

関連トピック

SIP フェデレーションの DNS 設定
SIP フェデレーテッド ドメインの追加
企業内の Microsoft OCS ドメインの追加

少し時間が経つとアベイラビリティと IM の交換を利用できなくなる

Cisco Jabber と Microsoft Office Communicator 間でアベイラビリティと IM を共有できますが、少し時間が経つと、相互にアベイラビリティを確認できなくなり、IM も交換できなくなります。

OCS/Access Edge：

1. Access Edge で、内部エッジと外部エッジ両方の FQDN が同じである可能性があります。また、同じ FQDN の 2 つの「A」レコードのエントリが DNS にあり、一方が外部エッジの IP アドレスに解決され、もう一方が内部エッジの IP アドレスに解決される可能性があります。

   Access Edge で、内部エッジの FQDN を変更し、更新したレコード エントリを DNS に追加します。元々 Access Edge の内部 IP に解決されていた 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設定し直します。

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を設定し直します。

DNS 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。

関連トピック

SIP フェデレーション用の外部サーバ コンポーネントの設定

在席ステータスの変更と IM 配信の遅延

Cisco Jabber と Microsoft Office Communicator 間で、IM and Presence サービス状態の変更の配信が遅れます。

IM and Presence サービス ノードで、Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context に [Disable Empty TLS Fragments（空の TLS フラグメントの無効化）] オプションが選択されていない可能性があります。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ インターフェイスにログインします。[システム（System）] > [セキュリティ（Security）] > [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 リンクをクリックします。

ステップ 3 TLS コンテキスト情報の領域で、[空の TLS フラグメントの無効化（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。

アベイラビリティ サブスクリプションを試行した後に 403 FORBIDDEN が返される

IM and Presence サービスで Microsoft Office Communicator ユーザのアベイラビリティにサブスクライブしようとすると、OCS サーバから 403 FORBIDDEN メッセージが送信されます。

Access Edge サーバで、IM and Presence サービス 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 サーバで、IM サービス プロバイダのリストに IM and Presence サービス ノードのエントリを追加します。Access Edge の DNS サーバに、IM and Presence サービス ノードのパブリック アドレスを指す IM and Presence サービス 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 サーバで、IM and Presence サービス ノードが [許可（Allow）] リストに追加されている可能性があります。Access Edge サーバで、IM and Presence サービス ノードを指す [許可（Allow）] リストからエントリを削除します。

関連トピック

SIP フェデレーション用の外部サーバ コンポーネントの設定

NOTIFY メッセージでのタイムアウト

NOTIFY メッセージを送信するときに IM and Presence サービスと Microsoft OCS 間で TCP を使用して直接フェデレーションが行われている場合、IM and Presence サービスがタイムアウトします。

場合によっては、IM and Presence サービス ノードで [レコード ルート ヘッダーでトランスポートを使用（Use Transport in Record-Route Header）] をイネーブルにする必要があります。

手順

ステップ 1 [Cisco Unified CM IM and Presence Administration] ユーザ 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 ボックスで、[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（Clusterwide）（SIP Parameters (Clusterwide)）] セクションで、[レコード ルート ヘッダのトランスポートを使用（Use Transport in Record-Route Header）] パラメータの [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 and Presence サービス証明書が受け入れられない

Access Edge が IM and Presence サービスからの証明書を受け入れません。

IM and Presence サービス/Cisco Adaptive Security Appliance 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 DNS サーバに、IM and Presence サービス ノードのパブリック アドレスを指す IM and Presence サービス ドメインの _sipfederationtls レコードがあることを確認します。[許可（Allow）] リストに IM and Presence サービスの FQDN を設定しない場合、IM and Presence サービス証明書の件名の CN が IM and Presence サービス ドメインの SRV レコードの FQDN に解決される必要があります。
2. FIPS が Access Edge でイネーブルであること（TLSv1 を使用すること）を確認します。
3. OCS でグローバルにフェデレーションがイネーブルであり、フロントエンド サーバでフェデレーションがイネーブルであることを確認します。
4. DNS SRV を解決できない場合、DNS が正しく設定され、Access Edge から type=srv の nslookup が実行されることを確認します。
5. Access Edge のコマンド プロンプトに nslookup と入力します。
6. set type=srv と入力します。
7. たとえば、次のように IM and Presence サービス ドメインの SRV レコードを入力します。**_sipfederationtls._tcp.abc.com**（この **abc.com** はドメイン名です）。SRV レコードが存在する場合、IM and Presence サービス/Cisco Adaptive Security Appliance の FQDN が返されます。

IM and Presence サービス/Cisco Adaptive Security Appliance：

IM and Presence サービスと Cisco Adaptive Security Appliance で暗号を確認します。[IM and Presence Service Administration] にログインし、[システム（System）] > [セキュリティ（Security）] > [TLS

コンテキスト設定（TLS Context Configuration）] > [デフォルト Cisco SIP プロキシ ピア認証 TLS コンテキスト（Default Cisco SIP Proxy Peer Auth TLS Context）]を選択し、「TLS_RSA_WITH 3DES_EDE_CBC_SHA」暗号が選択することを確認します。

関連トピック

SIP フェデレーション用の外部サーバ コンポーネントの設定
選択した TLS ピア サブジェクト リストへの TLS ピアの追加

OCS でフロントエンド サーバの起動に問題がある

OCS でフロントエンド サーバが起動しません。

OCS で、Access Edge のプライベート インターフェイスの FQDN が [承認されたホスト（Authorized Hosts）] のリストに定義されている可能性があります。OCS の [承認されたホスト（Authorized Hosts）] 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 のインストール時に、RTCService と RTCComponentService という 2 つの Active Directory ユーザ 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付与されますが、これら両方のアカウントでは、[パスワードを無期限にする（Password never expires）] オプションがデフォルトで選択されないため、パスワードは定期的に期限切れになります。OCS サーバで RTCService または RTCComponentService のパスワードをリセットするには、次の手順を実行します。

手順

ステップ 1 ユーザ アカウントを右クリックします。
ステップ 2 [パスワードをリセット（Reset Password）] を選択します。
ステップ 3 ユーザ 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（Account）] 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。

Access Edge に対してリモート デスクトップを実行できない

Windows XP で FIPS を有効にしている場合、Access Edge サーバに対してリモート デスクトップを実行できません。

これは、Microsoft の既知の問題です。この問題を回避するには、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 の URL に記載されている順に従って操作してください。

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