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

IM and Presence 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 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のエラー

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 CLI でドメインを設定し、IM and Presence 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 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 による IM and Presence ドメインの設定

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）
- Organizational Unit
- 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>,
OU=<organisational_unit>,O=<organisation_name>,C=<country>,St=<state>,L=<locality>
```

関連トピック

VeriSign 用の新しいトラストポイントを生成する

IM and Presence のドメインまたはホスト名を変更するときに SSL エラーが発生する

CLI から IM and Presence ドメインを変更すると、IM and Presence 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 ドメイン名を変更する場合、IM and Presence 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 と Cisco Adaptive Security Appliance（ASA）の間でのセキュリティ証明書交換

TLS プロキシ クラス マップの作成時にエラーが発生する

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_cup_to_foreignciscoasa(config-cmap)# match
 access-list ent_cup_to_foreign
ERROR: Specified ACL (ent_cup_to_foreign) either does not exist or its
type is not supported by the match command.
ciscoasa(config-cmap)# exit

ciscoasa(config)# class-map ent_foreign_to_cup
ciscoasa(config-cmap)# match access-list ent_foreign_to_cup
ERROR: Specified ACL (ent_foreign_to_cup) 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 サービスは起動しません。

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 ドメインを設定できます。 IM and Presence 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 ドメインを削除

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

アップグレード後の Cisco Adaptive Security Appliance に問題がある

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 <Cisco Adaptive Security Appliance 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。

```
tftpdnld
```

（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。

一般的な統合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

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。

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 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：

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

4. 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。 また、SIP プロキシ ドメインが、IM and Presence サーバが属するドメインに正しく設定されていない可能性があります。 SIP プロキシのデフォルトは、新規インストール時にセットアップしたドメインになります。

   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、ルートの種類を「domain」に設定し、リバース宛先パターンを設定する必要があります。たとえば、フェデレーテッド ドメインが abc.com の場合、宛先アドレス パターンを “.com.abc.*” に設定する必要があります。 スタティック ルートを IM and Presence の管理で設定するには、[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。

Cisco Jabber クライアント：

Cisco Jabber クライアントの DNS 設定が正しく設定されていない可能性があります。 クライアント マシンが正しい DNS を指していることを確認します。 Cisco Jabber クライアントからログアウトし、ログインします。

関連トピック

外部 Access エッジ インターフェイスの証明書の設定
IM and Presence での証明書の新規作成
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：

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 レコードが正しく設定されているかどうかを確認するには、IM and Presence と Access Edge の両方から type=srv の nslookup を実行します。

Access Edge：

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 または Cisco Adaptive Security Appliance の FQDN が返されます。
   IM and Presence：
4. リモート アクセス アカウントを使用して、ssh で IM and Presence サーバにログインします。
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：

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、ルートの種類を「domain」に設定し、リバース宛先パターンを設定する必要があります。たとえば、フェデレーテッド ドメインが “abc.com” の場合、宛先アドレス パターンを “.com.abc.*” に設定する必要があります。 スタティック ルートを IM and Presence の管理で設定するには、[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。
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。 IM and Presence の管理で [システム（System）] > [サービス パラメータ（Service Parameters）] を選択し、SIP Proxy サービスを選

択します。 画面の最後で、[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）] 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。 IM and Presence の管理で、[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
エンタープライズへの 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 フェデレーションに関する外部サーバ コンポーネントの設定

在席ステータスの変更と IM の配信が遅れる

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

IM and Presence サーバで、Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context に [空の TLS フラグメントの無効化（Disable Empty TLS Fragments）] 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 の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [TLS コンテキスト設定（TLS Context Configuration）] の順に選択します。

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 [空の TLS フラグメントの無効化（Disable Empty TLS Fragments）] をオンにします。

ステップ 4 [保存（Save）] をクリックします。

プレゼンスのサブスクリプションを試行すると 403 FORBIDDEN が返される

IM and Presence で Microsoft Office Communicator ユーザのプレゼンス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。

アクセス エッジ サーバで、IM and Presence サーバが 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。 アクセス エッジ サーバで、IM and Presence サーバのエントリを IM サービス プロバイダ リストに追加します。 Access Edge の DNS サーバに、IM and Presence サーバのパブリック アドレスを指す IM and Presence ドメインの _sipfederationtls レコードがあることを確認します。

または

アクセス エッジ サーバで、IM and Presence サーバが [許可（Allow）] リストに追加されている可能性があります。 アクセス エッジ サーバで、[許可（Allow）] リストから IM and Presence サーバを指すエントリを削除します。

関連トピック

SIP フェデレーションに関する外部サーバ コンポーネントの設定

NOTIFY メッセージでタイムアウトが発生する

NOTIFY メッセージを送信するときに IM and Presence がタイムアウトします（IM and Presence 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）。

場合によっては、IM and Presence サーバで [Record-Route ヘッダーで転送を使用する（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 の管理（Cisco Unified CM IM and Presence Administration）] > [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 [Cisco SIP Proxy] サービスを選択します。

ステップ 3 [SIP パラメータ（クラスタ全体）（SIP Parameters (Clusterwide)）] セクションで、[Record-Route ヘッダーで転送を使用する（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 4 [保存（Save）] をクリックします。

IM and Presence 証明書が受け入れられない

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

IM and Presence/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 IM プロバイダ リストに IM and Presence サーバのパブリック FQDN を含め、IM and Presence 証明書の件名の CN が一致することを確認します。 [許可（Allow）] リストに IM and Presence の FQDN を設定しない場合、IM and Presence 証明書の件名の CN が IM and Presence 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 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 または Cisco Adaptive Security Appliance の FQDN が返されます。

IM and Presence/Cisco Adaptive Security Appliance：

IM and Presence と Cisco Adaptive Security Appliance で暗号を確認します。 IM and Presence の管理で、[システム（System）] > [セキュリティ（Security）] > [TLS コンテキスト設定(TLS Context Configuration)] > [デフォルトの Cisco SIP Proxy 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 フェデレーションに関する外部サーバ 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 [パスワードのリセット（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）] をオンにします。
ステップ 7 [**OK**] をクリックします。

ログイン後に Cisco Jabber がオンラインにならない

ログイン後に、Cisco Jabber クライアントのステータスがオンラインになりません。

クライアント コンピュータが誤った DNS サーバを指している可能性があります。 クライアント PC で正しい DNS サーバを更新してから、もう一度 Cisco Jabber にログインします。

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 をイネーブルにしている場合、アクセス エッジ 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、既知の Microsoft 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

Cisco Unified Communications Manager Release 9.0(1) の IM and Presence サービスに対するドメイン間フェデレーション