CUCMの証明書の再生成

内容

概要

このドキュメントでは、Cisco Unified Communications Manager(CUCM)リリース8.X以降で証明書を再生成する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- *Real Time Monitoring Tool*(RTMT)
- CUCM証明書

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CUCMリリース8.X以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、Cisco Unified Communications Manager(CUCM)リリース8.X以降で証明書を再生成する手順について説明します。ただし、これは12.0以降のITLリカバリの変更を反映するものではありません。

RTMTのインストール

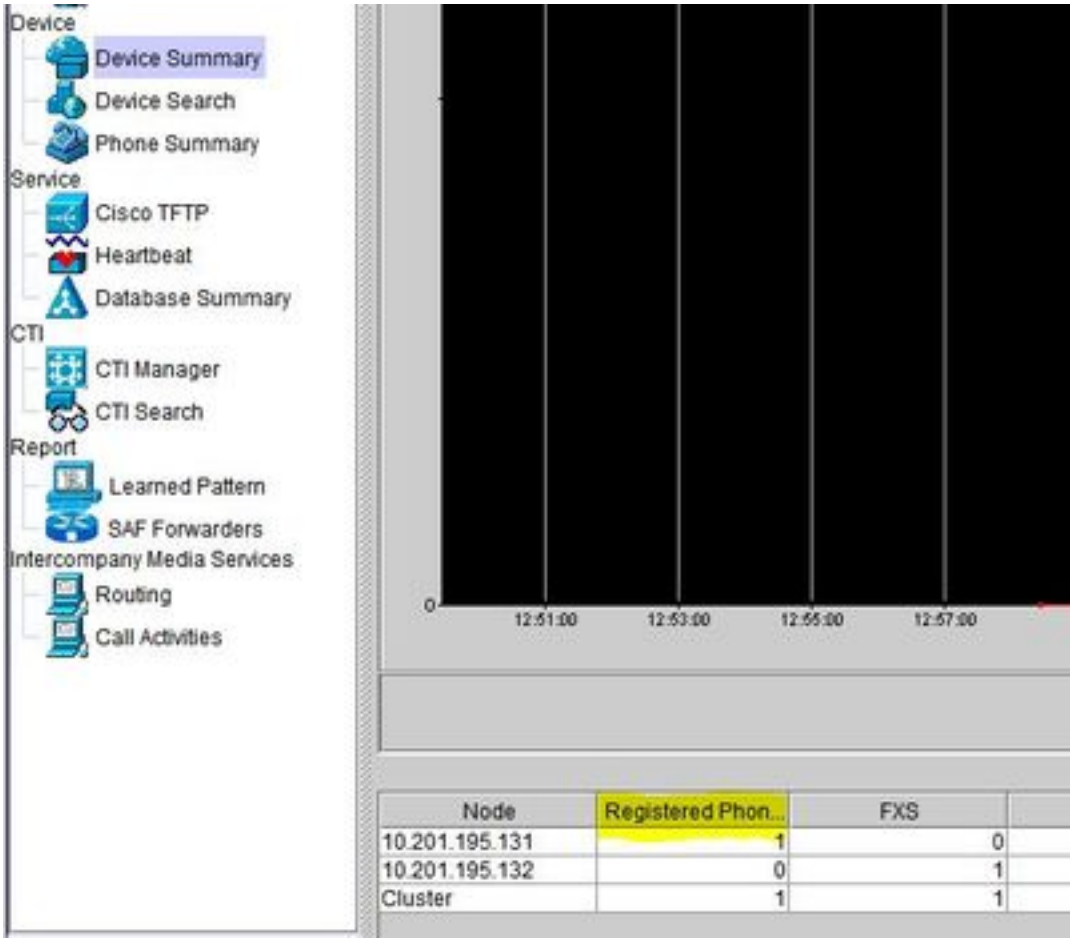
- Call ManagerからRTMTツールをダウンロードしてインストールします。 [Call Manager (CM) Administration]に移動します。 **アプリケーション>プラグイン>検索> Cisco Unified Real-Time Monitoring Tool - Windows > Download** インストールと起動

RTMTによるエンドポイントの監視

- RTMTを起動し、IPアドレスまたは完全修飾ドメイン名(FQDN)を入力し、次にユーザ名とパスワードを入力してツールにアクセスします。
- [Voice/Video] タブを選択します。[Device Summary] を選択します。 このセクションでは、登録されているエンドポイントの総数と、各ノードへの接続数を示しますエンドポイントのリセット中に監視して、次の証明書を再生成する前に登録を確認する

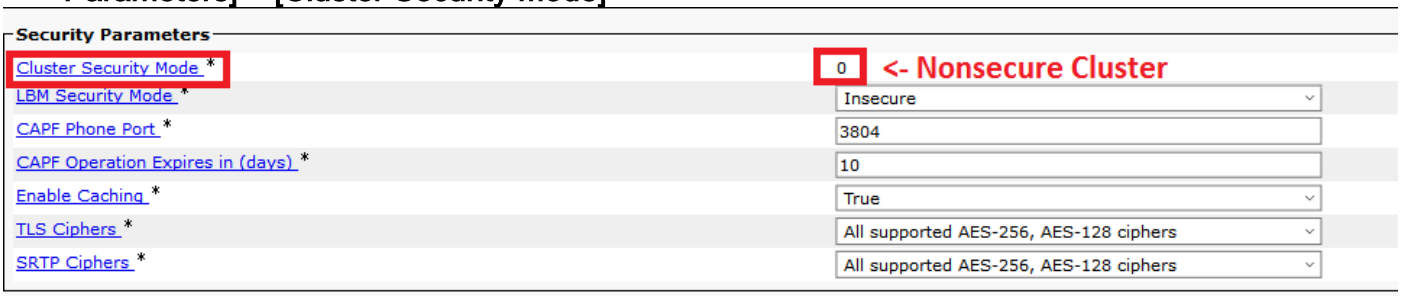
  ヒント：一部の証明書の再生成プロセスは、エンドポイントに影響する可能性があります。サービスの再起動と電話機の再起動が必要なため、通常の営業時間後にアクションプランを検討します。RTMTによる電話登録が強く推奨されることを確認します。

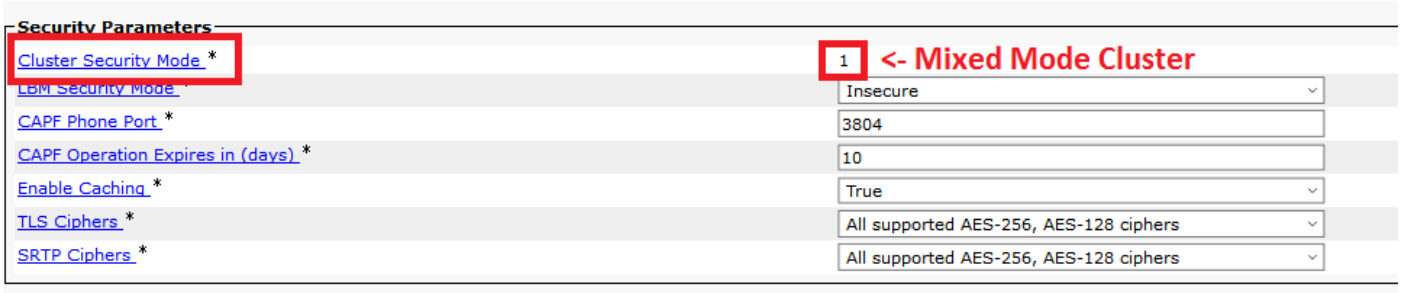
  警告：現在のITLの不一致があるエンドポイントでは、このプロセスの後に登録の問題が発生する可能性があります。 エンドポイントでのITLの削除は、再生成プロセスが完了し、他のすべての電話機が登録された後の一般的なベストプラクティスソリューションです。



クラスターが混合モードか非セキュアモードかを特定します

- [CM Administration]に移動します。 **[System] > [Enterprise Parameters] > [Security Parameters] > [Cluster Security Mode]**





証明書ストアによる影響

システム機能を正常に動作させるには、CUCMクラスタ全体ですべての証明書を更新することが重要です。証明書の期限が切れたり無効になったりすると、システムの通常の機能に大きな影響を与える可能性があります。影響は、システムの設定によって異なる場合があります。無効また

は期限切れの特定の証明書のサービスのリストを次に示します。

CallManager.pem

- 暗号化/認証された電話機が登録されない
- Trivial File Transfer Protocol(TFTP)が信頼されていない（電話機は署名付き設定ファイルやITLファイルを受け入れない）
- 電話サービスが影響を受ける可能性がある
- Secure Session Initiation Protocol(SIP)トランクまたはメディアリソース(会議ブリッジ、メディアターミネーションポイント(MTP)、Xcodersなど)が登録または機能しません。
- AXL 要求が失敗します。

Tomcat.pem

- 電話機は、社内ディレクトリなどのCUCMノードでホストされているHTTPサービスにアクセスできません
- CUCMには、クラスタ内の他のノードからサービスページにアクセスできないなど、さまざまなWeb問題が発生する可能性があります
- エクステンションモビリティ(EM)またはクラスタ間のエクステンションモビリティの問題
- シングルサインオン(SSO)
- UCCX(Unified Contact Center Express)が統合されている場合、CCX 12.5からのセキュリティ変更のため、Finesseデスクトップログインに影響を与えるため、UCCX tomcat-trustストアにCUCM Tomcat証明書（自己署名）またはTomcatルートおよび中間証明書（CA署名用）をアップロードする必要があります。

CAPF.pem

- 電話は電話VPN、802.1x、または電話プロキシを認証しません
- 電話機のローカルで有効な証明書(LSC)を発行できません。
- 暗号化された設定ファイルが機能しない

IPSec.pem

- ディザスタリカバリシステム(DRS)/ディザスタリカバリフレームワーク(DRF)が正しく機能しない
- ゲートウェイ(GW)から他のCUCMクラスタへのIPsecトンネルが機能しない

TVS（信頼検証サービス）

信頼検証サービス(TVS)は、デフォルトでセキュリティの主要コンポーネントです。TVSを使用すると、HTTPSが確立されたときに、Cisco Unified IP PhoneでEMサービス、ディレクトリ、MIDletなどのアプリケーションサーバを認証できます。

TVSには次の機能があります。

- 拡張性：Cisco Unified IP Phoneのリソースは、信頼する証明書の数の影響を受けません。
- 柔軟性：信頼証明書の追加または削除は、システムに自動的に反映されます。

- デフォルトのセキュリティ：非メディアおよび信号セキュリティ機能はデフォルトのインストールの一部であり、ユーザによる介入は必要ありません。

ITLおよびCTL

- ITLには、Call Manager TFTPの証明書ロール、クラスタ内のすべてのTVS証明書、および実行時のCertificate Authority Proxy Function(CAPF)が含まれます。
- CTLには、同じサーバ、CAPF、TFTPサーバ、および適応型セキュリティアプライアンス(ASA)ファイアウォール上で実行されるSystem Administrator Security Token(SAST)、Cisco CallManagerおよびCisco TFTPサービスのエントリが含まれています。TVSはCTLで参照されません。

証明書の再生成プロセス

> **注**：証明書を再生成する前に、すべてのエンドポイントの電源をオンにして登録する必要があります。そうでない場合は、接続されていない電話機でITLを削除する必要があります。

Tomcat証明書

サードパーティ証明書が使用されているかどうかを確認します。

1. クラスタ内の各サーバに移動します（Webブラウザの個別のタブで）。パブリッシャで始まり、サブスクライバが続きます。 [Cisco Unified OS Administration] > [Security] > [Certificate Management] > [Find] に移動します。
   Tomcatが「Self-signed certificate generated by system」と表示される場合は、[Description]列から確認します。Tomcatがサードパーティによって署名されている場合は、提供されているリンクに従って、Tomcatの再生後にこれらの手順を実行します。サードパーティ署名証明書については、『CCMAdmin Web GUI証明書のCUCMへのアップロード』を参照してください。
2. すべての証明書を表示するには、[Find] を選択します。 **Tomcat pem**証明書を選択します。開いたら、[Regenerate] を選択し、[Success]ポップアップが表示されるまで待ってからポップアップを閉じるか、戻って[Find/List] を選択します。
3. 後続の各サブスクライバで続行し、ステップ2の同じ手順に従って、クラスタ内のすべてのサブスクライバで完了します。
4. すべてのノードがTomcat証明書を再生成したら、すべてのノードでtomcatサービスを再起動します。パブリッシャから開始し、サブスクライバを続けます。 Tomcatを再起動するには、各ノードのCLIセッションを開き、コマンド**utils service restart Cisco Tomcat**を実行する必要があります。

```
admin:
admin:utils service restart Cisco Tomcat
 Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

5.次の手順は、CCX環境（該当する場合）から必要です。

- 自己署名証明書を使用する場合は、CUCMクラスタのすべてのノードからUnified CCX Tomcat信頼ストアにTomcat証明書をアップロードします。
- CA署名付き証明書またはプライベートCA署名付き証明書を使用する場合は、CUCMのルートCA証明書をUnified CCX Tomcat信頼ストアにアップロードします。
- CCXの証明書の再生成に関するドキュメントに記載されているように、サーバを再起動します。

参考資料:

- UCCXソリューション証明書管理ガイド
- Unified CCXヘルスチェックユーティリティ

IPSEC証明書

注：DRFのバージョン10.X以前のCUCM/Instant Messaging and Presence(IM&P) Master エージェントは、CUCMパブリッシャとIM&Pパブリッシャの両方で実行されます。DRF Localサービスは、加入者でそれぞれ実行されます。 バージョン10.X以降、DRF Master エージェントはCUCMパブリッシャでのみ実行され、CUCMサブスクライバ、IM&Pパブリッシャ、およびサブスクライバではDRFローカルサービスが実行されます。

注：ディザスタリカバリシステムは、Secure Socket Layer(SSL)ベースの通信を Master CUCMクラスタノード間のデータの認証と暗号化を行うエージェントとローカルエージェント。DRSは、公開/秘密キー暗号化にIPSec証明書を使用します。[Certificate Management]ページからIPSECトラストストア(hostname.pem)ファイルを削除すると、DRSが期待どおりに動作しなくなることに注意してください。IPSEC-trustファイルを手動で削除する場合は、IPSEC証明書をIPSEC信頼ストアにアップロードする必要があります。詳細については、『Cisco Unified Communications Managerセキュリティガイド』の証明書管理のヘルプページを参照してください。

1. クラスタ内の各サーバに移動します（Webブラウザの個別のタブで）。パブリッシャで始まり、サブスクライバが続きます。[Cisco Unified OS Administration] > [Security] > [Certificate Management] > [Find] に移動します。
   IPSEC PEM証明書を選択します。開いたら、[Regenerate] を選択し、[Success]ポップアップが表示されるまで待ってからポップアップを閉じるか、戻って[Find/List] を選択します。
2. 後続のサブスクライバで続行します。ステップ1と同じ手順に従い、クラスタ内のすべてのサブスクライバで完了します。
3. すべてのノードがIPSEC証明書を再生成したら、サービスを再起動します。
   パブリッシャの[Cisco Unified Serviceability] に移動します。 **[Cisco Unified Serviceability] > [Tools] > [Control Center - Network Services]**[Restart on] を選択します **Cisco DRF Master**service .サービスの再起動が完了したら、パブリッシャの**Cisco DRF Local Service**で**Restart**を選択し、サブスクライバで続行して**Cisco DRF Local Service**で**Restart**を選択します。

パブリッシャのIPSEC.pem証明書は有効であり、すべてのサブスクライバにIPSECトラストストアとして存在する必要があります。サブスクライバのIPSEC.pem証明書は、標準導入ではIPSECトラストストアとしてパブリッシャに存在しません。有効性を確認するには、PUBからのIPSEC.pem証明書のシリアル番号をSUBのIPSEC-trustと比較します。一致する必要があります。

CAPF証明書

警告：先に進む前に、クラスタが混合モードになっているかどうかを確認してください。「**クラスタが混合モードか非セキュアモードかを特定する**」の項を参照してください。

1. [Cisco Unified CM Administration] > [System] > [Enterprise Parameters] に移動します。セクション「セキュリティパラメータ」を確認し、「クラスタセキュリティモード」が0または1に設定されていることを確認します。値が0の場合、クラスタは非セキュアモードです。1の場合、クラスタは混合モードであり、サービスを再起動する前にCTLファイルを更新する必要があります。トークンとトークンレスリンクを参照してください。
2. クラスタ内の各サーバに移動します（Webブラウザの別のタブで）。最初にパブリッシャ、次に各サブスクライバの順に移動します。 [Cisco Unified OS Administration] > [Security] > [Certificate Management] > [Find] に移動します。**CAPF** PEM証明書**を選択**します。開いたら、[Regenerate] を選択し、[Success]ポップアップが表示されるまで待ってからポップアップを閉じるか、戻って[Find/List] を選択します
3. 後続のサブスクライバで続行します。ステップ2と同じ手順に従い、クラスタ内のすべてのサブスクライバで完了します。 クラスタが混合モードのみでCAPFが再生成された場合は、トークン（トークンレス）に進む前にCTLを更新します。クラスタが混合モードの場合、他のサービスを再起動する前に、Call Managerサービスも再起動する必要があります。
4. すべてのノードがCAPF証明書を再生成したら、サービスを再起動します。パブリッシャの[Cisco Unified Serviceability] に移動します。 **[Cisco Unified Serviceability] > [Tools] > [Control Center - Feature Services]**パブリッシャから開始し、アクティブな場合のみ**Cisco Certificate Authority Proxy Function Service**で**Restart**を選択します。
5. [Cisco Unified Serviceability] > [Tools] > [Control Center - Network Services] に移動します。パブリッシャから開始し、サブスクライバで続行し、**Cisco Trust Verification Service**で[Restart] を選択します。 [Cisco Unified Serviceability] > [Tools] > [Control Center - Feature Services] に移動します。パブリッシャから開始し、サブスクライバで続行し、アクティブな場所でのみ**Cisco TFTP Service**を再起動します。
6. すべての電話をリブートします。 **[Cisco Unified CM Administration] > [System] > [Enterprise Parameters]**[Reset] を選択すると、「**You are about to reset all devices in the system.この操作は元に戻せません。[Continue?]** で[OK] を選択し、[Reset] を選択します。

これで電話機がリセットされます。RTMTツールを使用して各自のアクションを監視し、リセットが成功したこと、およびデバイスがCUCMに再登録されたことを確認します。 電話機の登録が完了するまで待ってから、次の証明書に進みます。この電話登録プロセスには、時間がかかる場合があります。再生成プロセスの前に不正なITLを持っていたデバイスは、削除されるまでクラスタに登録し直さないことに注意してください。

CallManager証明書

警告：先に進む前に、クラスタが混合モードになっているかどうかを確認してください。「**クラスタが混合モードか非セキュアモードかを特定する**」セクションを参照してください。

警告：CallManager.PEM証明書とTVS.PEM証明書を同時に再生成しないでください。 これにより、クラスタ内のすべてのエンドポイントからITLを削除する必要があるエンドポイントにインストールされているITLと回復不能な不一致が発生します。CallManager.PEMのプロセス全体を終了し、電話機が再登録されたら、TVS.PEMのプロセスを開始します。

1. [Cisco Unified CM Administration] > [System] > [Enterprise Parameters] に移動します。 セクション「セキュリティパラメータ」を確認し、「クラスタセキュリティモード」が0または

1に設定されていることを確認します。値が0の場合、クラスタは非セキュアモードです。1の場合、クラスタは混合モードであり、サービスを再起動する前にCTLファイルを更新する必要があります。トークンとトークンレスリンクを参照してください。

2. クラスタ内の各サーバに移動します（Webブラウザの別のタブで）。最初にパブリッシャ、次に各サブスクライバの順に移動します。[Cisco Unified OS Administration] > [Security] > [Certificate Management] > [Find] に移動します。
[CallManager pem Certificate]を選択します。開いたら、[Regenerate] を選択し、[Success]ポップアップが表示されるまで待ってからポップアップを閉じるか、戻って[Find/List] を選択します。
3. 後続のサブスクライバで続行します。ステップ2と同じ手順に従い、クラスタ内のすべてのサブスクライバで完了します。 クラスタが混合モードのみであり、CallManager証明書が再生成された場合は、次に進む前にCTLを更新してください。トークン:トークンレス
4. パブリッシャCisco Unifiedサービスアビリティにログインします。 [Cisco Unified Serviceability] > [Tools] > [Control Center - Feature Services] に移動します。パブリッシャから開始し、サブスクライバで続行し、アクティブな**Cisco CallManager Service**を再起動します。
5. [Cisco Unified Serviceability] > [Tools] > [Control Center - Feature Services] に移動します。パブリッシャから開始し、サブスクライバで続行し、アクティブな場所でのみ**Cisco CTIManager Service**を再起動します。
6. [Cisco Unified Serviceability] > [Tools] > [Control Center - Network Services] に移動します。パブリッシャから開始し、サブスクライバで続行して、**Cisco Trust Verification Service**を再起動します。
7. [Cisco Unified Serviceability] > [Tools] > [Control Center - Feature Services] に移動します。パブリッシャから開始し、サブスクライバで続行し、アクティブな場所でのみ**Cisco TFTP Service**を再起動します。
8. すべての電話をリブートします。 **[Cisco Unified CM Administration] > [System] > [Enterprise Parameters]**[Reset] を選択すると、「**You are about to reset all devices in the system.この操作は元に戻せません。[Continue?]** で[OK] を選択し、[Reset] を選択します

これで電話機がリセットされます。RTMTツールを使用して各自のアクションを監視し、リセットが成功したこと、およびデバイスがCUCMに再登録されたことを確認します。 電話機の登録が完了するまで待ってから、次の証明書に進みます。この電話登録プロセスには、時間がかかる場合があります。再生成プロセスの前に不正なITLを持っていたデバイスは、ITLが削除されるまでクラスタに登録し直さないことに注意してください。

TVS証明書

> **警告：** CallManager.PEM証明書とTVS.PEM証明書を同時に再生成しないでください。 これにより、クラスタ内のすべてのエンドポイントからITLを削除する必要があるエンドポイントにインストールされているITLと回復不能な不一致が発生します。

> **注：**TVSは、Call Managerの代わりに証明書を認証します。この証明書を最後に再生成します。

クラスタ内の各サーバに移動します（Webブラウザの別のタブで）。最初にパブリッシャ、次に各サブスクライバの順に移動します。 [Cisco Unified OS Administration] > [Security] > [Certificate Management] > [**Find:**

- **TVS pem**証明書を選択します。
- 開いたら、[Regenerate] を選択し、[Success]ポップアップが表示されるまで待ってからポップアップを閉じるか、戻って[Find/List] を選択します。

1. 後続のサブスクライバで続行します。ステップ1と同じ手順に従い、クラスタ内のすべてのサブスクライバで完了します。 すべてのノードがTVS証明書を再生成したら、サービスを再起動します。 パブリッシャの**Cisco Unified** Serviceability**にログインします**。 [Cisco Unified Serviceability] > [Tools] > [Control Center - Network Services] に移動します。パブリッシャで、[Restart on Cisco Trust Verification Service] を選択します。サービスの再起動が完了したら、サブスクライバで続行し、**Cisco Trust Verification Service**を再起動します。
2. パブリッシャから開始し、サブスクライバで続行し、アクティブな**Cisco TFTP Service**のみを再起動します。
3. すべての電話をリブートします。 [Cisco Unified CM Administration] > [System] > [Enterprise Parameters] **の順に選択します。**[Reset] を選択すると、「**You are about to reset all devices in the system.この操作は元に戻せません。[Continue?]** で[OK] を選択し、[Reset] を選択します。

これで電話機がリセットされます。RTMTツールを使用して各自のアクションを監視し、リセットが成功したこと、およびデバイスがCUCMに再登録されたことを確認します。 電話機の登録が完了するまで待ってから、次の証明書に進みます。この電話登録プロセスには、時間がかかる場合があります。再生成プロセスの前に不正なITLを持っていたデバイスは、ITLが削除されるまでクラスタに登録し直さないことに注意してください。

ITLRecovery証明書

注：ITLRecovery証明書は、デバイスが信頼できるステータスを失ったときに使用されます。証明書はITLとCTLの両方に表示されます（CTLプロバイダーがアクティブな場合）。デバイスの信頼状態が失われた場合は、非セキュアクラスタに対してコマンド**utils itl reset localkey**を使用し、ミックスモードクラスタに対してコマンド**utils ctl reset localkey**を使用できます。Call Managerバージョンのセキュリティガイドを読み、ITLRecovery証明書の使用方法と、信頼できるステータスを回復するために必要なプロセスについて理解します。クラスタが2048のキー長をサポートするバージョンにアップグレードされ、クラスタサーバ証明書が2048に再生成され、ITLRecoveryが再生成されておらず、現在のキー長が1024である場合、ITL回復コマンドは失敗し、ITLRecoveryメソッドは使用されません。

1. クラスタ内の各サーバに移動します（Webブラウザの別のタブで）。最初にパブリッシャ、次に各サブスクライバの順に移動します。 [Cisco Unified OS Administration] > [Security] > [Certificate Management] > [Find] に移動します。
   ITLRecovery pem証明書を選択します。開いたら、[Regenerate] を選択し、[Success]ポップアップが表示されるまで待ってからポップアップを閉じるか、戻って[Find/List] を選択します。
2. 後続のサブスクライバで続行します。ステップ2と同じ手順に従い、クラスタ内のすべてのサブスクライバで完了します。
3. すべてのノードがITLRecovery証明書を再生成した後、次の順序でサービスを再起動する必要があります。 混合モードの場合は、トークン – トークンレスに進む前にCTLを更新します。パブリッシャ**Cisco Unifiedサービスアビリティ**にログインします。 [Cisco Unified Serviceability] > [Tools] > [Control Center - Network Services] に移動します。パブリッシャで、[Restart on Cisco Trust Verification Service] を選択します。 サービスの再起動が完了したら、サブスクライバで続行し、**Cisco Trust Verification Service**を再起動します。

4. パブリッシャから開始し、サブスクライバで続行し、アクティブなCisco TFTP Serviceのみを再起動します。
5. すべての電話をリブートします。 [Cisco Unified CM Administration] > [System] > [Enterprise Parameters][Reset] を選択すると、「You are about to reset all devices in the system.この操作は元に戻せません。[Continue?] で[OK] を選択し、[Reset] を選択します。
6. 電話機のリセット中に新しいITL/CTLがアップロードされるようになりました。

期限切れの信頼証明書の削除

注：削除する必要がある、不要になった、または期限が切れた信頼証明書を特定します。CallManager.pem、tomcat.pem、ipsec.pem、CAPF.pem、およびTVS.pemを含む5つの基本証明書は削除しないでください。信頼証明書は、必要に応じて削除できます。次に再起動するサービスは、それらのサービス内のレガシー証明書の情報をクリアするように設計されています。

1. [Cisco Unified Serviceability] > [Tools] > [Control Center - Network Services] に移動します。ドロップダウンからCUCMパブリッシャを選択します。Stop Certificate Change Notificationを選択します。クラスタ内のすべてのCall Managerノードに対して、この手順を繰り返します。IMPサーバがある場合： ドロップダウンメニューからIMPサーバを1つずつ選択し、[Stop Platform Administration Web Services] と[Cisco Intercluster Sync Agent]を選択します。
2. [Cisco Unified OS Administration] > [Security] > [Certificate Management] > [Find] に移動します。
   期限切れの信頼証明書を検索します。(バージョン10.X以降では、有効期限でフィルタリングできます。10.0より前のバージョンでは、特定の証明書を手動で識別するか、受信した場合はRTMTアラートを使用して識別する必要があります)。同じ信頼証明書を複数のノードに表示できます。各ノードから個別に削除する必要があります。削除する信頼証明書を選択します (ポップアップが表示されるか、同じページで証明書に移動するかによって、バージョンが異なります) 。 Deleteを選択します。(「この証明書を完全に削除しようとしています」というポップアップが表示されます)。OKを選択します。
3. 削除するすべての信頼証明書に対して、このプロセスを繰り返します。
4. 完了時に、削除された証明書に直接関連するサービスを再起動する必要があります。このセクションでは、電話機をリブートする必要はありません。 Call ManagerとCAPFはエンドポイントに影響を与える可能性があります。 Tomcatの信頼性:コマンドラインからTomcatサービスを再起動します (「Tomcat」の項を参照) capf-trust:cisco Certificate Authority Proxy Functionを再起動します (「CAPF」の項を参照) 。エンドポイントをリブートしないでください。CallManager-trust:CallManager Service/CTIManager (「CallManager」セクションを参照) エンドポイントをリブートしないでください。 エンドポイントに影響を与え、再起動を引き起こします。Ipsecの信頼性:DRF Master/DRFローカル (IPSECセクションを参照) 。TVS (自己署名) には信頼証明書がありません。
5. ステップ1で停止したサービスを再起動します。

確認

この設定では、確認手順は使用できません。

トラブルシュート

この設定では、トラブルシューティング手順は使用できません。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。