CUCM 電話証明書（LSC/MIC）のための Q.A

目次

概要

この資料はいくつかの Cisco Unified Communications Manager（CUCM）電話証明書のための質疑応答を取り扱っています。 電話証明書の速いビューはここにあります。

製造業者インストール済み証明書（MIC）:

名前が示すと同時に、電話は MIC とプレインストールされ、これは管理者によって削除され/修正することができません。 CA SHA2 を製造する認証局（CA） 証明書 CAP-RTP-001、CAP-RTP-002、Cisco_Manufacturing_CA および Cisco は CUCM で MIC を信頼するためにプレインストールされます。 MIC は有効性が生成されるに関して MIC CA 傾斜としてあれば切れれば使用することができません、

ローカルで固有の証明書（LSC）:

LSC は Cisco Unified Communications Manager プロキシ 機能（CAPF）プライベートキーによって認証局（CA）署名する Cisco IP Phone のための公開キーを所有しています。 それは電話でデフォルトでインストールされていません。 管理者は LSC を完全な制御をコントロールします。 CAPF CA 認証は電話に必要とされて時はいつでも次々とできます新しい LSC を発行再生することができます。

電話証明書のためのよくある使用とは何か。

電話証明書のためのいくつかのよくある使用はここにあります

/アップグレードするかのための CAPF と電話間、削除するか、または解決しますインストール

確立します電話で CAPF/アップグレードを用いる接続をインストールするか、削除するか、または証明書を解決するために電話をかけて下さい。 電話 Certficate が既存の認証（LSC への優位）によってへのまたは既存の認証（MIC への優位）によって設定 される 認証局 （CA） プロキシ 機能（CAPF）情報の下で CAPF の接続をとき認証モード確立するのに使用されています。

既存の認証（LSC への優位）によって: 電話は LSC を CAPF と認証するのに使用します。 それは LSC がインストールされていない場合 MIC を使用します。 インストールは理由「無効 LSC」と使用された証明書においての問題がある場合失敗します。 例は、LSC のための署名された CA CAPF 信頼で利用できません。 他の証明書 方式を使用してまたはそのような障害ケースのためのヌルストリングによって認証モードをアップデートして下さい。

既存の認証（MIC への優位）によって: 電話は MIC を CAPF と認証するのに使用します。

Trasnsport 層 セキュリティ（TLS）接続のための CallManager と電話間

電話は LSC か MIC を CallManager の TLS 接続を確立するのに使用します。 CallManager は CallManager 信頼のチェックによる電話によって示された Certficate を検証します。 それぞれ CAPF 証明書は LSC のために CallManager 信頼および MIC のために Cisco 製造 CA で利用可能でなければなりません。

802.1X 認証のための電話と認証サーバ間

CAPF/Manufacturing CA 証明書は Cisco Secure Access Control Server （ACS）または Identity Services Engine （ISE）のような認証サーバにアップロードされます。 認証サーバはアップ ロードされた証明書を時それ現在証明書電話を認証するのに使用します（LSC か MIC）。

VPN のための電話間の証明書によって基づく認証に関してはおよび Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェア（ASA）

CAPF/Manufacture CA 証明書は ASA で信頼電話現在の LIC/MIC がそれのチェックによって、ASA それを検証するとき、アップロードされます。

LSC および MIC が時接続に LSC か MIC を明示的に選択する、

あらゆる方法ありますか。

接続にかどうか LSC か MIC 選択するオプション無し。 LSC がインストールされている場合、電話は LSC を使用します。 電話は LSC がインストールされていない場合 MIC を使用します。

LSC がない場合の Console エントリ:

SECD: - PXY_NO_LSC: LSC はのための[SCCP]、MIC を試みません

LSC がある場合の Console エントリ:

SECD: - PXY_CERT_CIPHER: [SCCP]、[TLSv1]、証明書[LSC]

LSC または MIC の選択は CAPF と電話/でアップグレードするか間でだけ可能性のある、削除するか、または解決しますインストール。

原因は何を新しいクラスタに移動すると LSC インストール済み電話保護されたプロファイルの登録されていませんですか。

これは電話のために既に古いクラスタからの LSC を持っているそれら起こる場合があります。 MIC および LSC が両方時、LSC が TLS 接続を確立するのに使用されています。 TLS は新しい CUCM に CallManager 信頼のこの LSC のための CA がないので確立することができません。

コンソール ログはどの証明書が TLS を確立するのに使用されているか示します。 エントリの下で LSC が使用されることを示します。

3469 ない 00:01:31.935298 SECD: - PXY_CERT_CIPHER: [SCCP]、[TLSv1]、証明書[LSC]、暗号 [AES256-SHA:AES128-SHA]

コンソール ログのそのような壊れるケースのための「未知 CA」の SSL3_Alert: -

3486 ERR 00:01:31.938954 SECD: -STATE_SSL3_ALERT: SSL3 アラート[読まれる]: [致命的]: [未知 CA

この問題を解決する方法の 1 つはありましたり、電話を非セキュア プロファイルを使用して登録されていて得ましたりそして既存の LSC を削除します。 LSC を新しいクラスタからインストールしそして保護されたプロファイルを使用して電話を登録して下さい。 それはまた可能性のある LSC をインストールしないで MIC を使用して登録されている保護されたプロファイルの電話があるためにです。

電話がそれを認証されたか、または暗号化された保護されたプロファイルを使用して登録されていて得ることができるようにインストールされる LSC があることを必要としますか。

いいえ。 LSC がインストールされていない場合、電話は MIC を CUCM への TLS 接続を確立するのに使用します。

4878 WRN 15:47:34.756063 SECD: - PXY_NO_LSC: LSC 無しのための[SCCP]、試み MIC。

認証されることは必須ことそれぞれデバイスセキュリティ プロファイルのデバイスセキュリティ モードまたは暗号化された/アップグレード/削除インストールするために LSC ですか。

それはデフォルトの基準値非セキュア プロファイルを使用してデバイスセキュリティでモードが非セキュアであるところに必須、それ余りにすることができますではないです。

それは必須電話に LSC をインストールするミックス モードにあるクラスタですか。

それは必須ではないです。 LSC インストール/削除は時でさえ非セキュアのクラスタ セキュリティモードすることができます。

そこに LSC においての問題すぐにテストする方法電話によって使用されますか。

電話管理者ページへ行くことによって電話の 1 の LSC を削除して下さい。 これは MIC を使用するために電話を強制します。 すべてが LSC をうまく MIC とそれからトラブルシューティング続行すれば。

トラブルシューティングのための電話証明書を得る方法か。

デバイス/電話の下で解決するために証明書 オペレーションを設定 して下さい。 ヒット保存はそれから構成を適用します。 証明書 オペレーション ステータスを**成功を解決するために**見るために待って下さい。 実時間監視 ツール (RTMT) から **Cisco プロキシ 機能**ログを**認証局 (CA)** 集めて下さい。 それは電話からの証明書が含まれています。

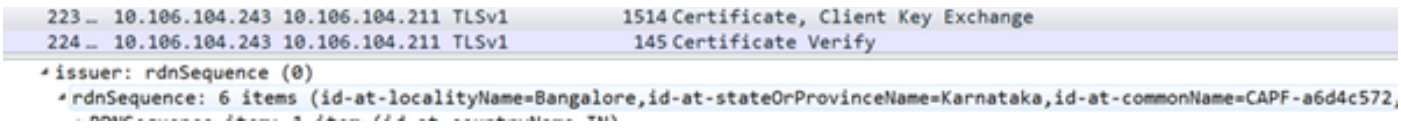
電話の LSC か MIC 使用された確立するが CallManager の TLS 接続である場合パケットキャプチャから確認する方法か。

電話再始動を力バーしているパケットキャプチャを集めて下さい。

証明書を、Client 鍵 交換メッセージ チェックして下さい。 IP Phone から送信 される 証明書を確認して下さい。

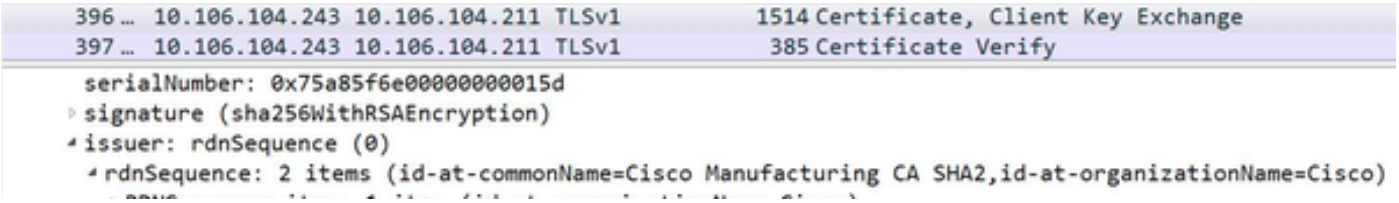
例 LSC:

LSC に関しては、CAPF CN は発行元 フィールドで見られます。 それぞれ CAPF ルートは CallManager 信頼にあるなります。



例 MIC:

MIC に関しては、発行元 フィールドの CA を製造する Cisco。 それぞれルートCA は CallManager 信頼にあるなります。



認証モードの重要性とは認証局（CA）プロキシ 機能（CAPF）情報の下に何か。 CUCM と電話間の TLS 接続のための重要性か。

それはだけ//でオペレーションを削除し、のための電話と CAPF 間の認証方式解決しますアップグレード インストール。 それは CUCM と電話間の TLS 接続のための重要性を持っていません。

CAPF 証明書の後で考えるべき電話のための基本的な LSC オペレーションとは何再生されたとか。

このセクションは LSC を発行するのにオフライン CA が使用されていないアイドル状態のシナリオをカバーします。

CallManager の TLS 接続

CallManager 信頼から前の CAPF 証明書を削除する前に電話で新しい LSC をインストールするために確認して下さい。 CallManagerサービスの再始動に先行している前の CAPF 証明書を削除してそれにこの CAPF 証明書によって発行される LSC がある電話に登録問題を引き起こして下さい。

CAPF 信頼の LSC オペレーション

CAPF 信頼から前の CAPF 証明書を削除する前に電話で新しい LSC をインストールするために確認して下さい。 **既存の認証（LSC への優位）による**認証モードを使用してインストール/削除のような LSC オペレーションはそれらにこの CAPF 証明書によって発行される LSC がある電話のためのエラー **無効 LSC** と失敗します。

802.1X 認証のための電話と認証サーバ間

アップ ロードされる新しい CAPF 証明書および電話が LSC を新しい CAPF によって発行されて得るまで認証サーバから前の CAPF 証明書を削除しないために確認して下さい。

ASA と電話間

電話が ASA に新しい LSC およびアップ ロードされた新しい CAPF CA 認証を得るまで ASA から前の CAPF 証明書を削除しないために確認して下さい。

CAPF 証明書を再生するために続かれるべきステップについては証明書再生を*参照して下さい。*

関連情報

- Cisco IP Phone 証明書およびセキュアコミュニケーション
- 802.1X 設計の指針のための IP テレフォニー
- Cisco Unified Communications Manager セキュリティ ガイド