Unified CCE Solution： サード パーティ CA証明（バージョン 11.x）を入手してアップロードするプロシージャ

目次

概要

この資料は Finesse、Cisco Unified Intelligence Center（CUIC）間の HTTPS 接続を確立し、サーバ データ（LD）住むために生成されるサードパーティベンダーから Certification Authority（CA）認証を得、インストールするために手順を詳しく説明することを向けます。

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。

- Cisco Unified Contact Center Enterprise（UCCE）
- Cisco Live データ（LD）
- Cisco Unified Intelligence Center（CUIC）
- Cisco Finesse
- 証明される CA

使用するコンポーネント

資料で使用される情報は UCCE ソリューション 11.0(1) バージョンに基づいています。

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、各手順が及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

HTTPS を、CUIC およびライブ データ サーバは Finesse 間のセキュアコミュニケーションのために使用するために、セキュリティ 認証 セットアップ必要です。 デフォルトでこれらのサーバは使用するまたは顧客は認証局 （CA） 署名入り認証を手に入れ、インストールできます自己署名 certifcates を提供します。 これらの CA 証明書は VeriSign のようなサードパーティベンダーから GeoTrust、Thawte 得る、ことができましたりまたは internaly 生成 することができます。

設定

Finesse の HTTPS 通信のための認証を設定して、CUIC およびライブ データ サーバはこれらのステップを必要とします:

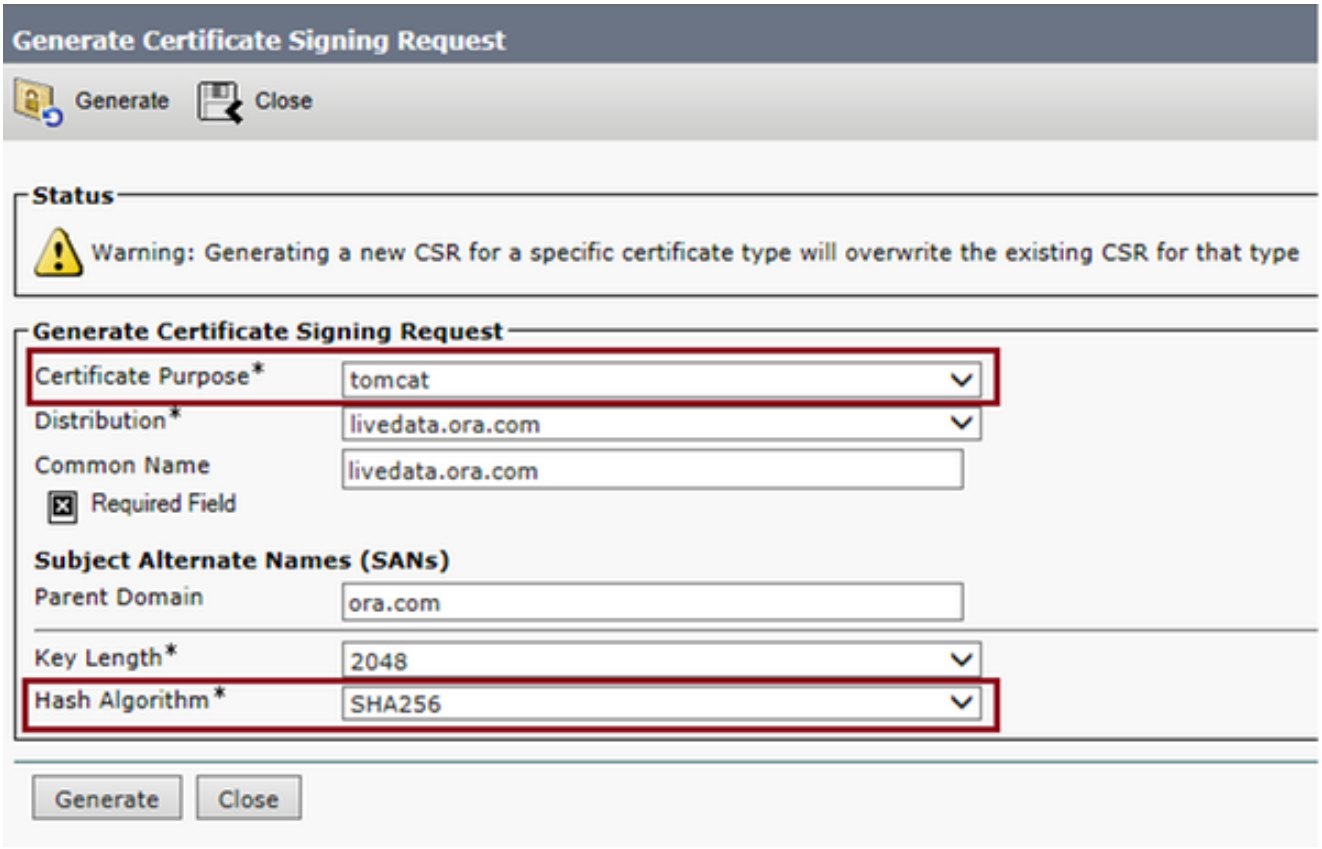
1. 証明書署名要求（CSR）の生成とダウンロード。
2. CSR を使用して、認証局からのルート、中間（該当する場合）、およびアプリケーション証明書を取得します。
3. サーバへの証明書のアップロード。

ステップ 1.生成するおよびダウンロード証明書署名要求（CSR）。

1. CSR を生成し、ダウンロードするためにここに記述されているステップは Finesse のため同じ、CUIC であり、ライブ データは断絶します。

2. **Cisco Unified Communications オペレーティング システム管理 ページを**示された URL を使用して開き、インストールプロセスの間に作成される OS 管理者アカウントと署名して下さい
   https://FQDN:8443/cmplatform

3. イメージに示すように証明書署名要求（CSR）を生成して下さい:

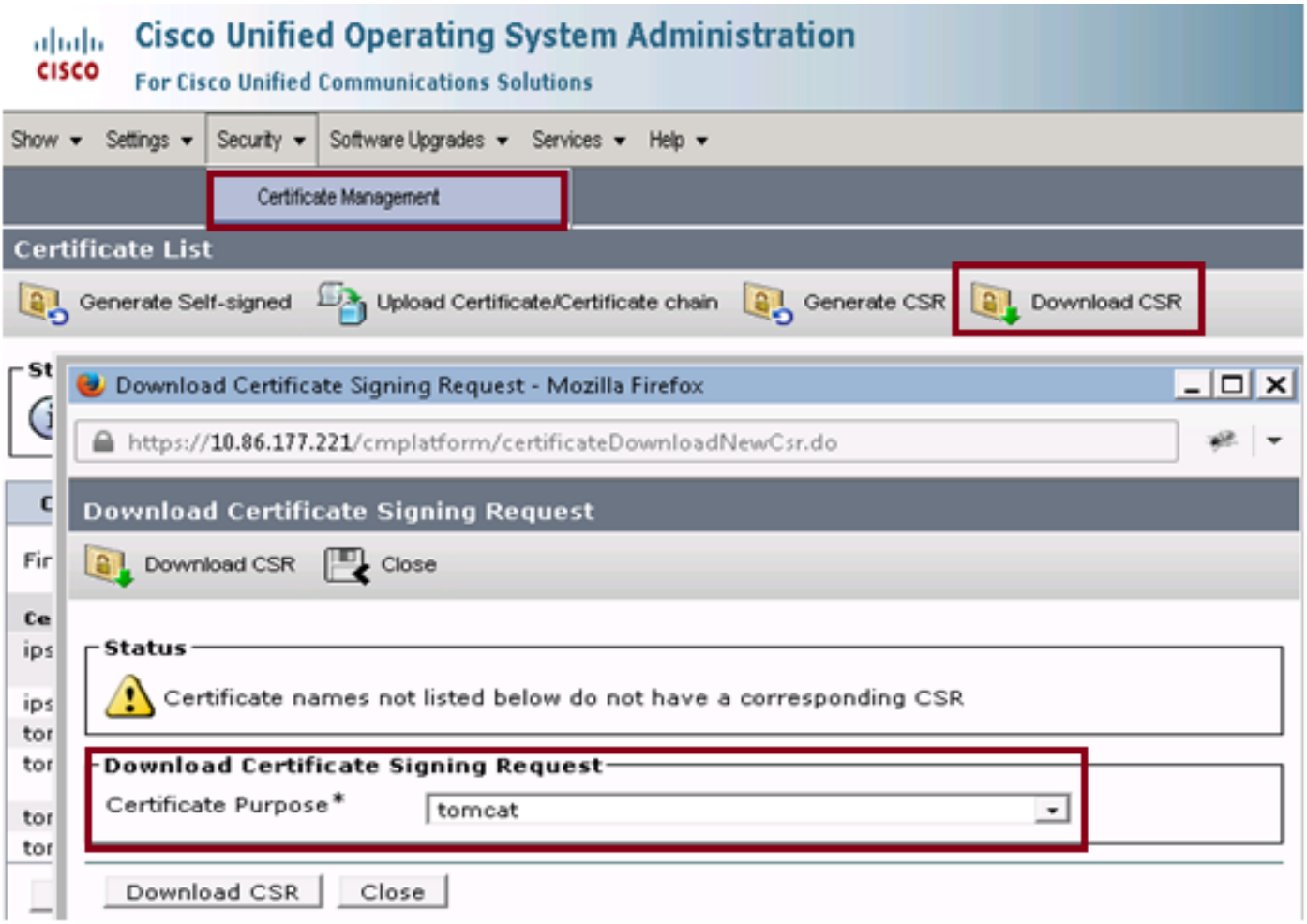


ステップ 1.**セキュリティ > Certificate Management > 生成する CSR** へのナビゲート。呼び出します。 [Certificate Purpose Name] ドロップダウン リストから、[tomcat] を選択します。ステップ 3.ビジネス上の必要に depeding ハッシュ アルゴリズムおよび変調長さを選択して下さい。

-変調長さ: 2048 \ハッシュ アルゴリズム: SHA256 は推奨されます

ステップ 4. **CSR を**『Generate』 をクリック して下さい。**注:** ビジネスは認証対象代替名（SAN）親 ドメイン フィールドがドメイン名でそして一杯になるように要求したら資料「Finesse のサード パーティ 署名入り認証においての SAN 問題」の問題アドレスを理解しておいて下さい。

4. イメージに示すように証明書署名要求（CSR）をダウンロードして下さい:



ステップ 1.**セキュリティ > Certificate Management > ダウンロード CSR** へのナビゲート。
呼び出します。 [Certificate Name] ドロップダウン リストから、[tomcat] を選択します。
ステップ 3. **CSR を**『Download』 をクリック して下さい。

注:

> **注:** 認証局（CA）のための CSR を得るために URL **https://FQDN:8443/cmplatform** を使用してセカンダリサーバの前述のステップを実行して下さい

ステップ 2.ルートを、中間物得て下さい（applicableStep なら 5.および認証局（CA）からのアプリケーション 認証。

1. VeriSign、Thawte、GeoTrust 先祖などのようなサード パーティ Certifcate 機関にプライマリおよびセカンダリサーバ 証明書署名要求（CSR）情報を提供します

2. certifcate 機関から 1 つはプライマリおよび secondory サーバのための次の証明書 チェーンを受け取る必要があります。

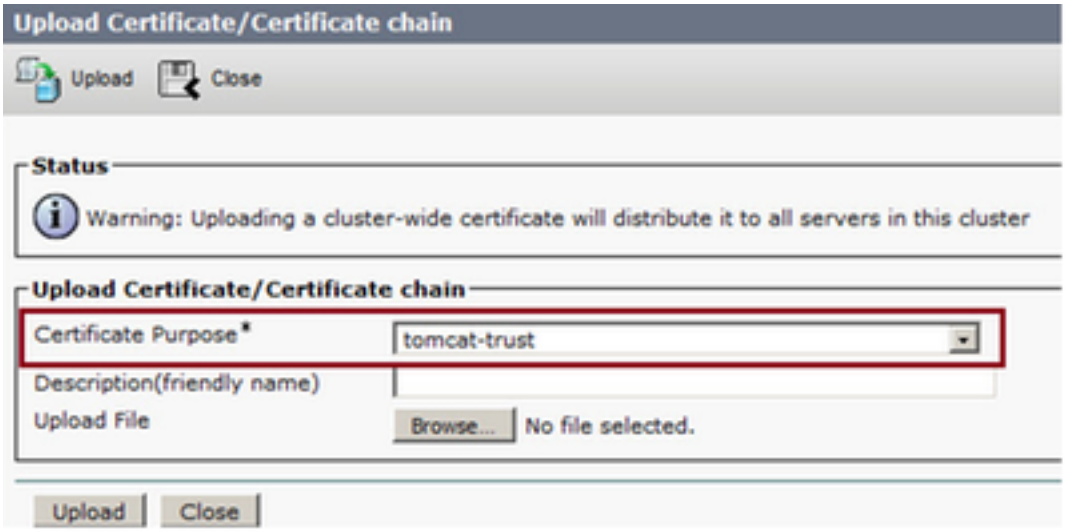
- **Finesse サーバ**： 認証定着させ、中間物、（オプションの）アプリケーション
- **CUIC サーバ**： 認証定着させ、中間物、（オプションの）アプリケーション
- **ライブ データ サーブ**: 認証定着させ、中間物、（オプションの）アプリケーション

ステップ 3.サーバへのアップロード認証。

このセクションは方法で証明書 チェーンを Finesse で、CUIC 正しくアップロードしデータ サー

バ住む記述します。

Finesse サーバ

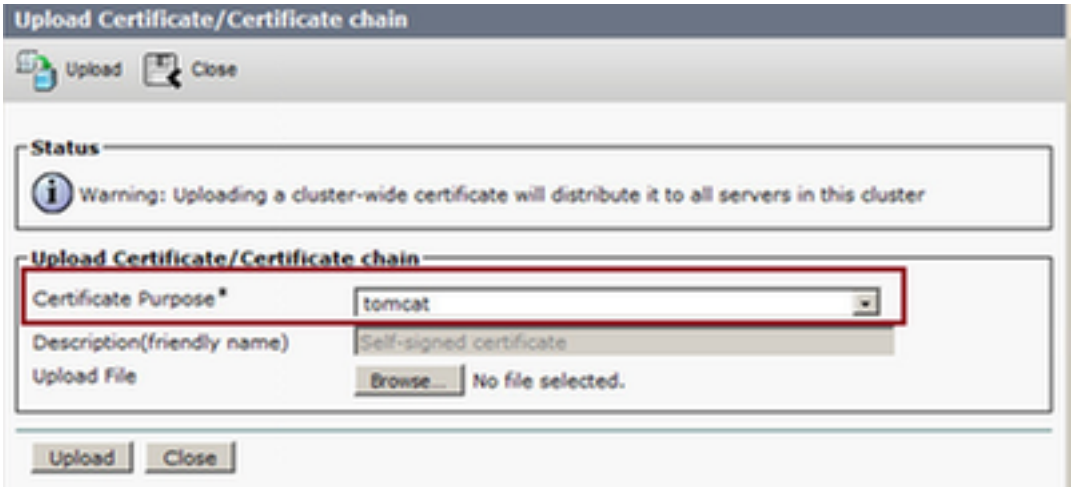


1. これらのステップの助けによってプライマリ Finesse サーバのルート証明をアップロードして下さい:

   ステップ 1： プライマリ サーバ Cisco Unified Communications オペレーティング システム管理 ページ、**セキュリティ > Certificate Management > アップ ロード認証**へのナビゲート。
   呼び出します。 [Certificate Name] ドロップダウン リストから、[tomcat-trust] を選択します。
   ステップ 3 [Upload File] フィールドで、[browse] をクリックし、ルート証明書ファイルを参照します。
   ステップ 4.ファイルを『Upload』 をクリック して下さい。

2. これらのステップの助けによって Fineese プライマリ サーバの中間認証をアップロードして下さい:

   ステップ 1.中間 certififcate のアップロードのステップはステップ 1.に示すようにルート証明と同じです。
   呼び出します。 プライマリ サーバ Cisco Unified Communications オペレーティング システム管理 ページ、**セキュリティ > Certificate Management > アップ ロード認証**へのナビゲート。
   ステップ 3 [Certificate Name] ドロップダウン リストから、[tomcat-trust] を選択します。
   ステップ 4 アップ ロード File フィールドで、中間証明書ファイルに『Browse』 をクリックし、参照して下さい。
   ステップ 5. 『Upload』 をクリック して下さい。**注:** Tomcat 信頼ストアがプライマリの間でルートをアップロードするためにおよび複製されると同時にセカンダリサーバ必要ではないですまたはセカンダリへの中間物認証はサーバをうまく解決します。
3. イメージに示すようにプライマリ Finesse サーバアプリケーション 認証をアップロードして下さい:



ステップ 1： [Certificate Name] ドロップダウン リストから、[tomcat] を選択します。呼び出します。 アップ ロード File フィールドで、アプリケーション 証明書ファイルに『Browse』 をクリック し、参照して下さい。
ステップ 3.ファイルをアップロードするために『Upload』 をクリック して下さい。

4. セカンダリ Fineese サーバアプリケーション 認証をアップロードして下さい。
   このステップで自身のアプリケーション 認証のためのセカンダリサーバのステップ 3 に言及されているように同じプロセスに従って下さい。

5. この場合サーバを再起動できます。
   プライマリおよびセカンダリ Finesse サーバの CLI にアクセスし、サーバを再起動するためにコマンド **utils システム 再始動を**入力して下さい。

CUIC サーバ (証明書 チェーンで現在の中間認証を仮定しない)

1. プライマリ CUIC サーバのルート証明をアップロードして下さい。

   ステップ 1： プライマリ サーバ Cisco Unified Communications オペレーティング システム 管理 ページ、**セキュリティ > Certificate Management > アップ ロード認証/証明書 チェーン**へのナビゲート。
   呼び出します。 [Certificate Name] ドロップダウン リストから、[tomcat-trust] を選択します。
   ステップ 3 [Upload File] フィールドで、[browse] をクリックし、ルート証明書ファイルを参照します。
   ステップ 4.ファイルを『Upload』 をクリック して下さい。**注:** Tomcat 信頼ストアがプライマリの間でセカンダリ CUIC サーバにルート証明をアップロードするためにおよび複製されると同時にセカンダリサーバ必要ではないです。

2. アップロード プライマリ CUIC サーバアプリケーション 認証。

   ステップ 1： [Certificate Name] ドロップダウン リストから、[tomcat] を選択します。
   呼び出します。 アップ ロード File フィールドで、アプリケーション 証明書ファイルに『Browse』 をクリック し、参照して下さい。
   ステップ 3.ファイルを『Upload』 をクリック して下さい。
3. セカンダリ CUIC サーバアプリケーション 認証をアップロードして下さい。

自身のアプリケーション 認証のためのセカンダリサーバのステップ（２）で既述のとおりに同じプロセスに従って下さい

4. **サーバの再起動**
   プライマリおよびセカンダリ CUIC サーバの CLI にアクセスし、サーバを再起動するためにコマンド**「utils システム 再始動」を**入力して下さい。
   注: CA 機関が中間認証が含まれている証明書 チェーンをセクションによってが CUIC サーブに同様に適当である Finesse サーバで述べられるステップ提供すれば。

ライブ データ サーバ

1. ライブ データ サーバで手順認証をアップロードすることは証明書 チェーンによってまたは CUIC サーバうまく解決するために同一です。

2. プライマリ ライブ データ サーバのアップロード ルート証明。

   ステップ 1： プライマリ サーバ Cisco Unified Communications オペレーティング システム管理 ページ、**セキュリティ > Certificate Management > アップ ロード認証**へのナビゲート。
   呼び出します。 [Certificate Name] ドロップダウン リストから、[tomcat-trust] を選択します。
   ステップ 3 [Upload File] フィールドで、[browse] をクリックし、ルート証明書ファイルを参照します。
   ステップ 4. 『Upload』 をクリック して下さい。

3. プライマリ ライブ データ サーバの中間認証をアップロードして下さい。

   ステップ 1.中間 certififcate のアップロードのステップはステップ 1.に示すようにルート証明と同じです。
   呼び出します。 プライマリ サーバ Cisco Unified Communications オペレーティング システム管理 ページ、**セキュリティ > Certificate Management > アップ ロード認証**へのナビゲート。
   ステップ 3 [Certificate Name] ドロップダウン リストから、[tomcat-trust] を選択します。
   ステップ 4 アップ ロード File フィールドで、中間証明書ファイルに『Browse』 をクリックし、参照して下さい。
   ステップ 5. 『Upload』 をクリック して下さい。
   注: Tomcat 信頼ストアがプライマリの間でセカンダリ ライブ データ サーバにルートか中間物認証をアップロードするためにおよび複製されると同時にセカンダリサーバ必要ではないです。
4. アップロード プライマリ ライブ データ サーバアプリケーション 認証。

   ステップ 1： [Certificate Name] ドロップダウン リストから、[tomcat] を選択します。
   呼び出します。 アップ ロード File フィールドで、アプリケーション 証明書ファイルに『Browse』 をクリック し、参照して下さい。
   ステップ 3. 『Upload』 をクリック して下さい。

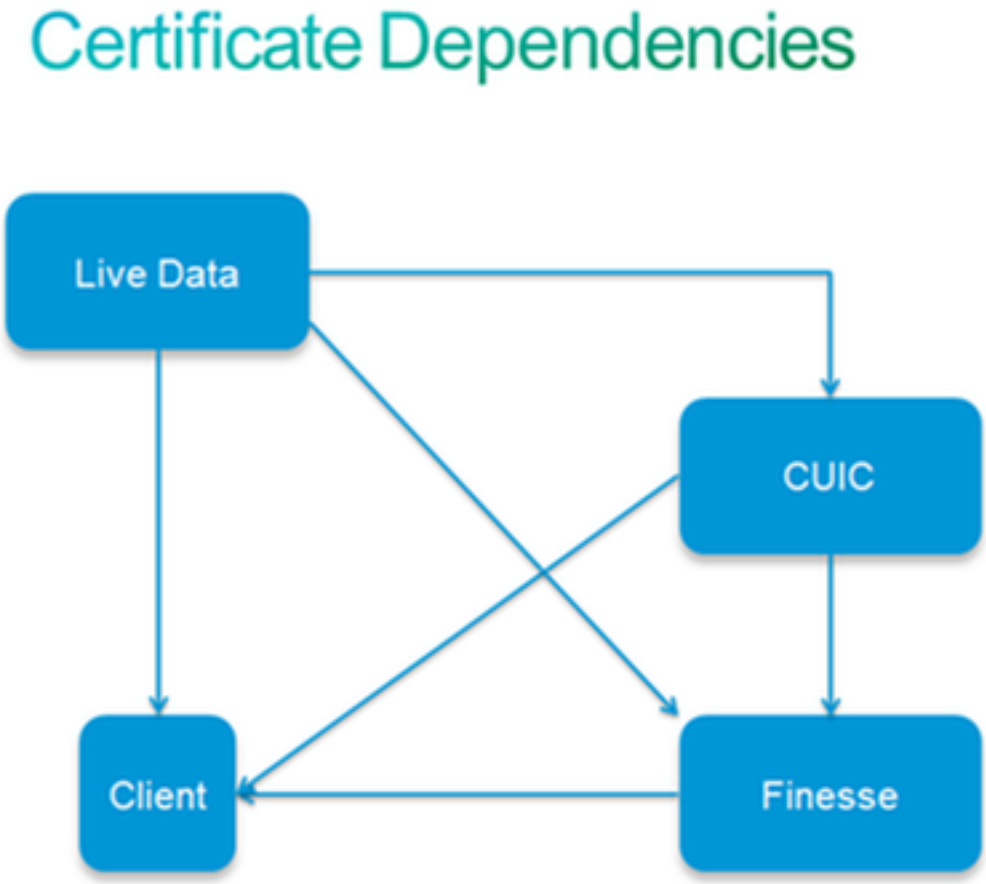
5. セカンダリ ライブ データ サーバアプリケーション 認証をアップロードして下さい。

自身のアプリケーション 認証のための secondory サーバの同じステップにの（4）前述のように従って下さい。

6. **サーバの再起動**
   プライマリおよびセカンダリ Finesse サーバの CLI にアクセスし、サーバを再起動するためにコマンド**「utils システム 再始動」を**入力して下さい。

データ サーバ 認証 依存関係は住んでいます

ライブ データ サーバとして相互に作用し、サーバを、イメージに示すように CUIC とありますこれらのサーバ間に認証 依存関係がうまく解決します:



サード パーティ CA 認証 チェーンに関してルートおよび中間物認証は組織のすべてのサーバのため同じです。 その結果きちんとはたらく Live データ サーバのために Finesse および CUIC サーバがそこにロードされるルートおよび中間物認証をきちんと Tomcat 信頼コンテナーで備えていることを確認しなければなりません。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。