統一された CCE ソリューション: サード パーティ CA 証明書 (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 ） 証明書を得、インストールするために必要となるステップ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。

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 ネットワークがライブである場合、あらゆるステップの潜在的影響を理解することを確かめて下さい。

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 証明書設定必要です。 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 コミュニケーションのための証明書を設定して、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:

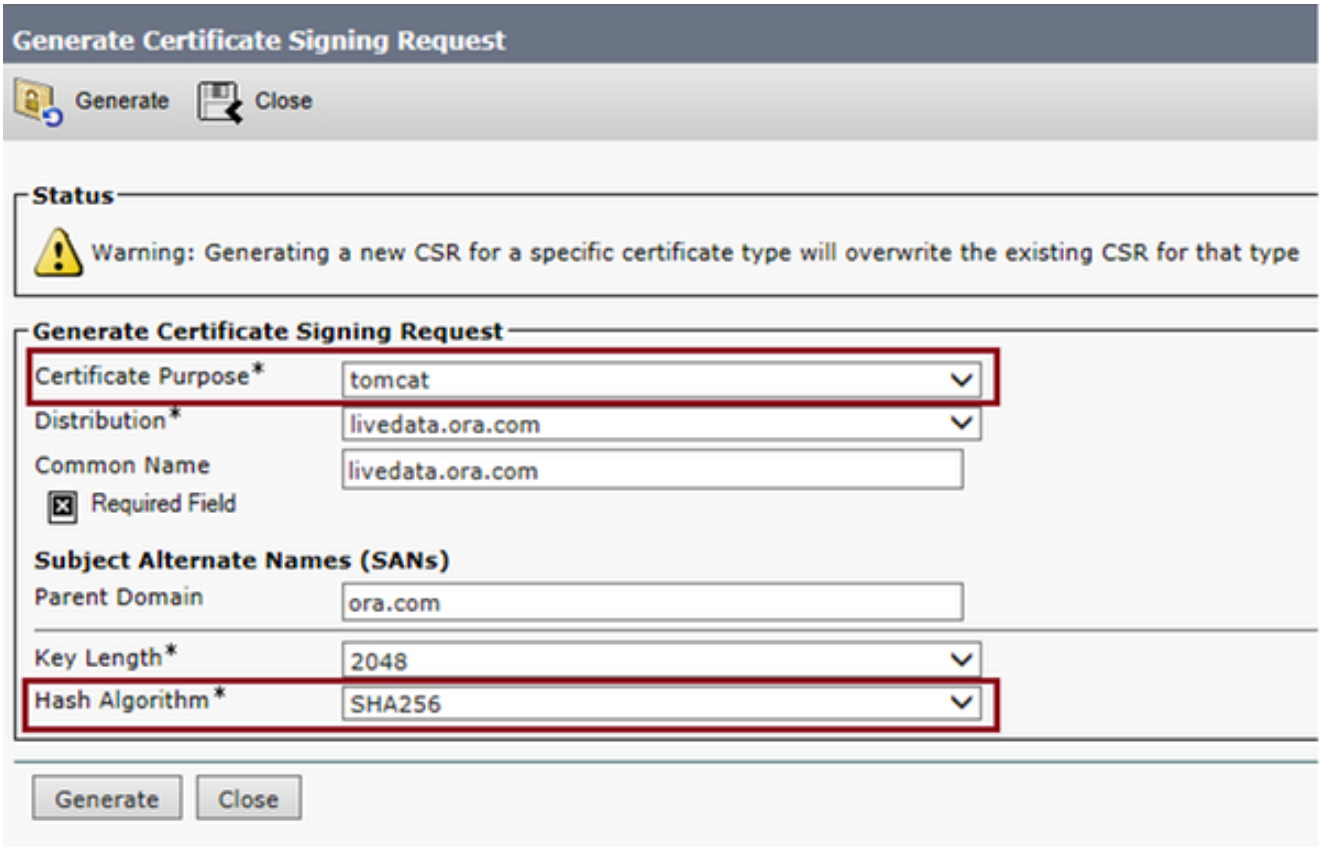
1. 生成するおよびダウンロード証明書署名要求（CSR）。
2. CSR を使用して認証局（CA）からのルート、中間物（適当であれば）およびアプリケーション 証明書を得て下さい。
3. サーバに証明書をアップ ロードして下さい。

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:

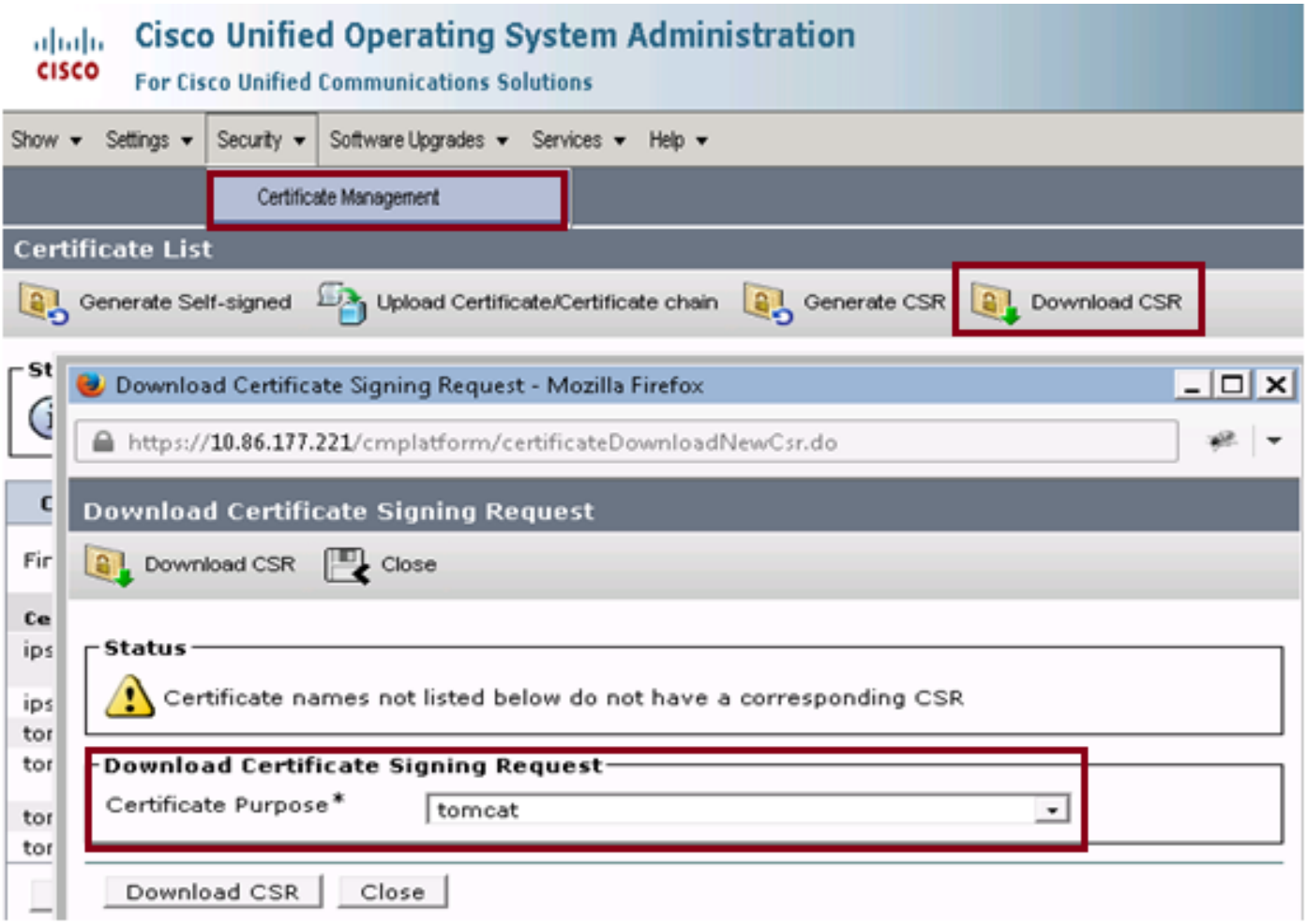


ステップ 1.**セキュリティ > Certificate Management > 生成する CSR** にナビゲートして下さい。呼び出します。 証明書目的名前ドロップダウン リストから、Tomcat を選択して下さい。ステップ 3.ビジネス上の必要に depeding ハッシュ アルゴリズムおよびキー長を選択して下さい。

-キー長: 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 Domain 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** にナビゲートして下さい。
呼び出します。 証明書名前ドロップダウン リストから、Tomcat を選択して下さい。
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 証明書。

1. VeriSign、Thawte、GeoTrust 等のようなサード パーティ Certifcate 権限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。

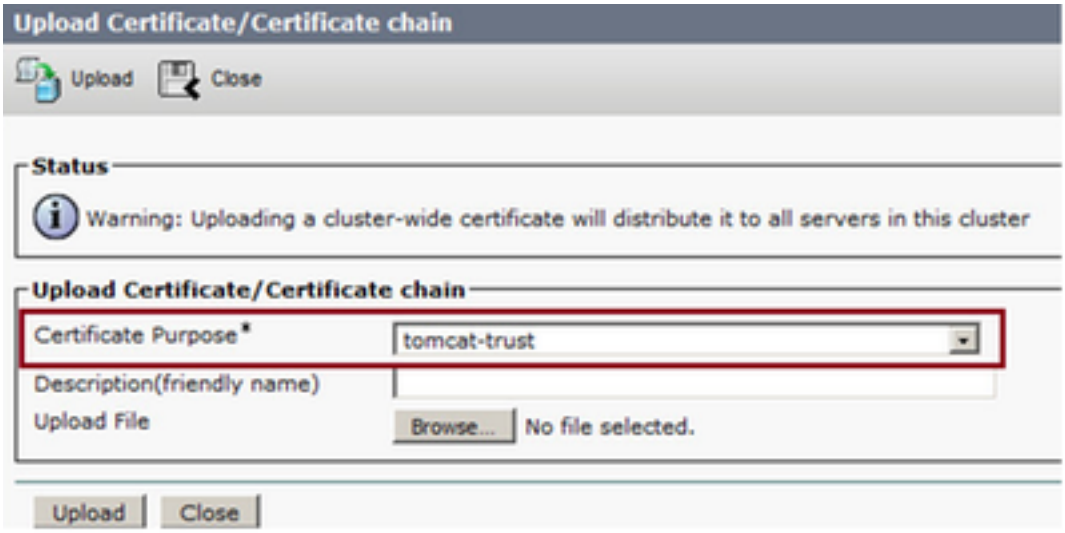
2. certifcate 権限から 1 つはプライマリおよび secondory サーバのための次の証明書 チェーンを受け取る必要があります。

- **Finesse サーバ: 証明書定着させ、中間物、（オプションの）アプリケーション**
- **CUIC サーバ: 証明書定着させ、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: 証明書定着させ、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 ロード証明書。

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

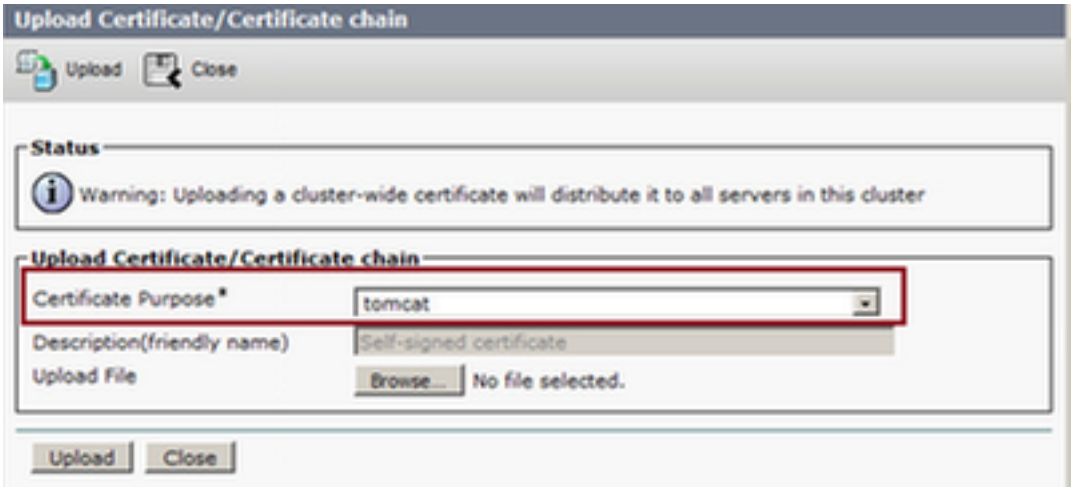


1. これらのステップの助けによってプライマリ Finesse サーバのルート証明をアップ ロードして下さい:

   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 ページで、**セキュリティ > Certificate Management > アップ ロード証明書**にナビゲートして下さい。
   呼び出します。 証明書名前ドロップダウン リストから、Tomcat 信頼を選択して下さい。
   ステップ 3 アップ ロード File フィールドで、ルート証明ファイルに『Browse』 をクリックし、参照して下さい。
   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 サーバの中間証明書をアップ 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 ページで、**セキュリティ > Certificate Management > アップ ロード証明書**にナビゲートして下さい。
   ステップ 3 証明書名前ドロップダウン リストから、Tomcat 信頼を選択して下さい。
   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技巧サーバにルートか中間物証明書をアップ 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。
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 証明書をアップ ロードして下さい:



ステップ 1： 証明書名前ドロップダウン リストから、Tomcat を選択して下さい。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 証明書をアップ 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 証明書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証明書を仮定しない)

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 ページで、**セキュリティ > Certificate Management > アップ ロード証明書/証明書 チェーン**にナビゲートして下さい。
呼び出します。 証明書名前ドロップダウン リストから、Tomcat 信頼を選択して下さい。
ステップ 3 アップ ロード File フィールドで、ルート証明ファイルに『Browse』 をクリックし、参照して下さい。
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 証明書。

ステップ 1： 証明書名前ドロップダウン リストから、Tomcat を選択して下さい。
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 証明書をアップ ロードして下さい。
自身のアプリケーション 証明書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. サーバを再起動して下さい
   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 権限が中間証明書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 サーブにまた適当である 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. ステップはライブ データ サーバで証明書をアップ ロードするためにです証明書 チェーンによって Finesse か CUIC サーバと同一含みました。

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 ページで、**セキュリティ > Certificate Management > アップ ロード証明書**にナビゲートして下さい。
   呼び出します。 証明書名前ドロップダウン リストから、Tomcat 信頼を選択して下さい。
   ステップ 3 アップ ロード File フィールドで、ルート証明ファイルに『Browse』 をクリックし、参照して下さい。
   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 サーバの中間証明書をアップ 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 ページで、**セキュリティ > Certificate Management > アップ ロード証明書**にナビゲートして下さい。
   ステップ 3 証明書名前ドロップダウン リストから、Tomcat 信頼を選択して下さい。
   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証明書をアップ 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 証明書。

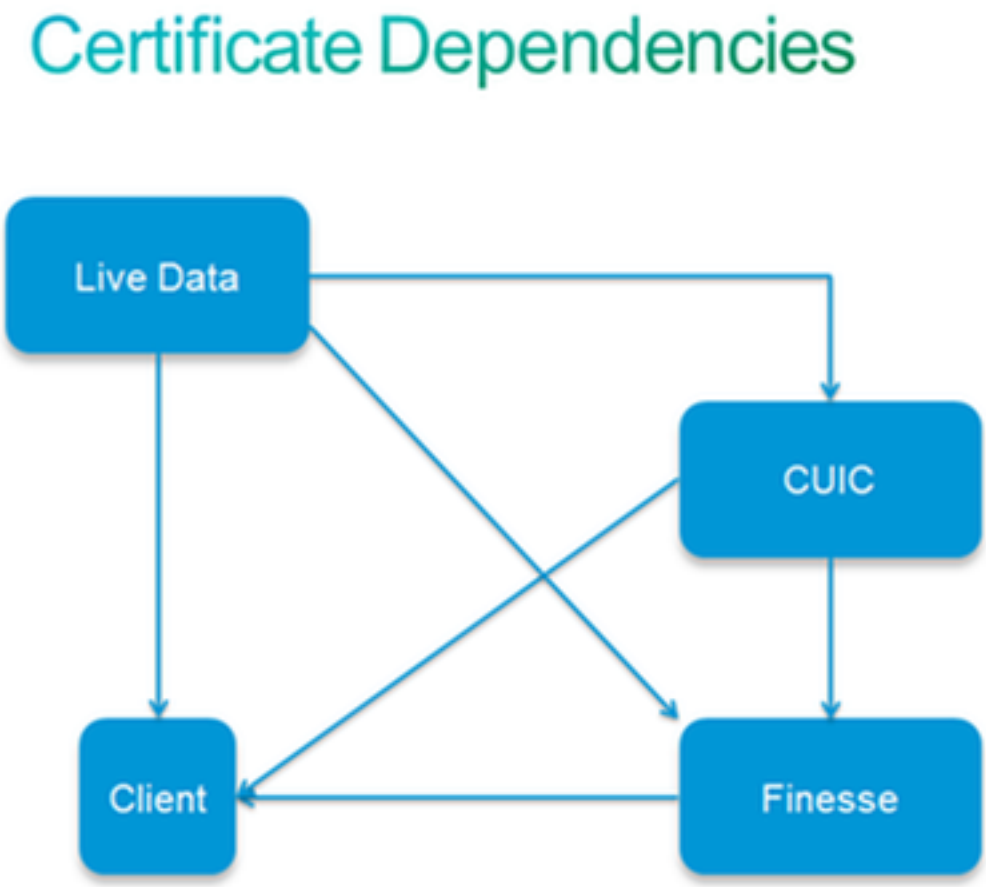
   ステップ 1： 証明書名前ドロップダウン リストから、Tomcat を選択して下さい。
   呼び出します。 アップ ロード File フィールドで、アプリケーション 証明書ファイルに『Browse』 をクリック し、参照して下さい。
   ステップ 3. 『Upload』 をクリック して下さい。

5. セカンダリ ライブ データ サーバアプリケーション 証明書をアップ ロードして下さい。
   自身のアプリケーション 証明書のための 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. サーバを再起動して下さい
   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 証明書 依存関係は住んでいます

ライブ データ サーバとして、イメージに示すように CUIC および Finesse サーバによってありますこれらのサーバ間に証明書 依存関係が相互に作用しています:



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証明書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証明書をきちんと Tomcat 信頼容器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。