Solution d'Unified CCE : Procédure pour obtenir et télécharger de tiers Certificats CA (version 11.x)

Contenu

Introduction

Ce document vise à expliquer en détail les étapes impliquées pour obtenir et installer un certificat de l'autorité de certification (CA), généré d'un fournisseur tiers pour établir une connexion HTTPS entre la finesse, le centre d'intelligence de Cisco Unified (CUIC), et pour vivre des serveurs des données (LD).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Contact Center Enterprise (UCCE)
- Données vivantes de Cisco (LD)
- Centre d'intelligence de Cisco Unified (CUIC)
- Cisco Finesse
- CA diplômée

Composants utilisés

Les informations utilisées dans le document sont basées sur la version de la solution UCCE 11.0(1).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle étape.

Informations générales

Afin d'utiliser HTTPS pour la communication protégée entre la finesse, CUIC et serveurs de données vivants, installation de Certificats de Sécurité est nécessaire. Par défaut ces serveurs fournissent les certifcates auto-signés qui sont utilisés ou les clients peuvent obtenir et installer l'Autorité de certification (CA) les Certificats signés. Ces CERT CA peuvent être obtenus d'un fournisseur tiers comme Verisign, Thawte, GeoTrust ou peuvent être produits internaly.

Configurez

Installant le certificat pour la transmission HTTPS dans la finesse, CUIC et serveurs de données vivants exigent ces étapes :

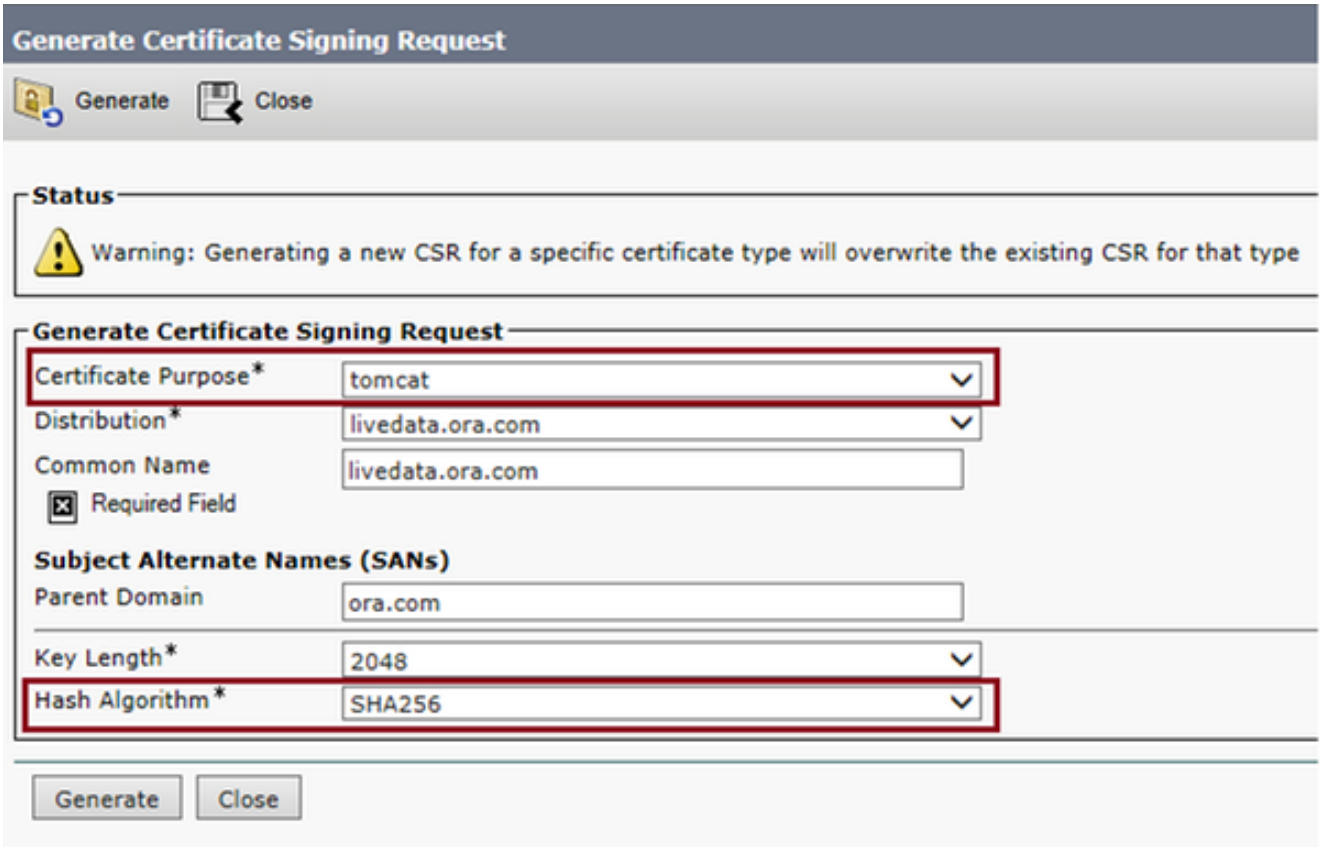
1. Générez et téléchargez la demande de signature de certificat (CSR).
2. Obtenez le certificat de racine, d'intermédiaire (si c'est approprié) et d'application de l'autorité de certification utilisant le CSR.
3. Certificats de téléchargement aux serveurs.

Étape 1. Générez et téléchargez la demande de signature de certificat (CSR).

1. Les étapes décrites ici pour générer et télécharger le CSR est mêmes pour la finesse, CUIC et les données vivantes divisent.

2. Ouvrez la page **du système d'exploitation de gestion de Cisco Unified Communications** utilisant l'URL indiqué et connectez-vous avec le compte d'admin de SYSTÈME D'EXPLOITATION créé pendant le processus d'installation
https://FQDN:8443/cmplatform

3. Générez la demande de signature de certificat (CSR) suivant les indications de l'image :

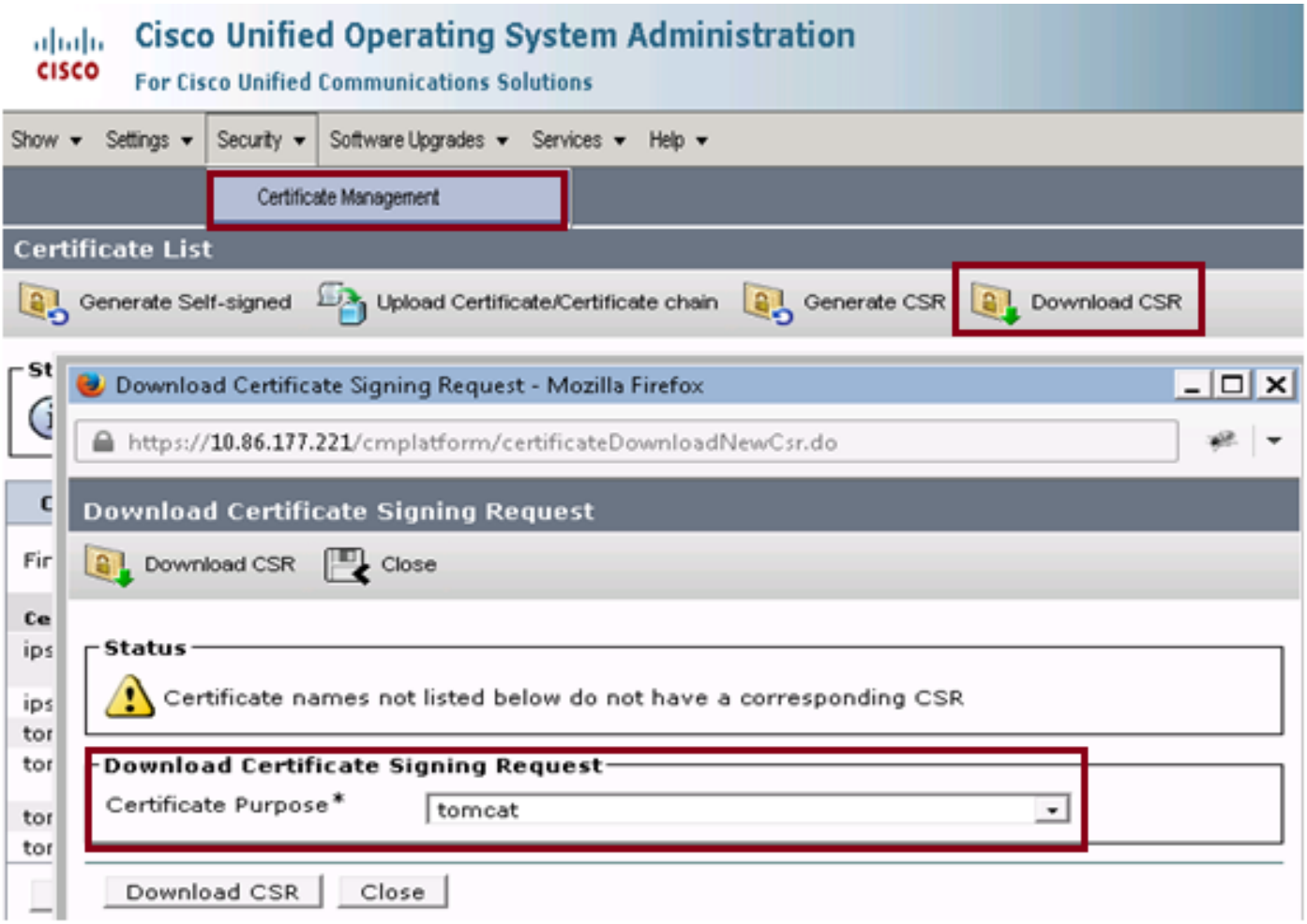


Étape 1. Naviguez vers la **Gestion de Sécurité > de certificat > génèrent le CSR**.Étape 2. De la liste déroulante de nom de but de certificat, chat choisi.Étape 3. Algorithme de hachage choisi et longueur principale depeding sur les besoins d'affaires.

- Longueur principale : 2048 \ algorithme de hachage : SHA256 est recommandé

Étape 4. Le clic **génèrent le CSR**.Remarque: Si l'entreprise exige le parent soumis de noms secondaires (sans) que le champ de domaine à remplir de nom de domaine satisfont alors se rende compte des adresses de question dans le document [« sans la question avec un certificat signé de tiers dans la finesse ».]

4. Téléchargez la demande de signature de certificat (CSR) suivant les indications de l'image :



Étape 1. Naviguez vers le **CSR de Sécurité > de Gestion > de téléchargement de certificat**.
Étape 2. De la liste déroulante de nom de certificat, chat choisi.
Étape 3. Cliquez sur Download le **CSR**.

Remarque:

> Remarque: Exécutez les étapes mentionnées ci-dessus sur le serveur secondaire employant l'URL **https://FQDN:8443/cmplatform** pour obtenir des CSR pour l'autorité de certification

Étape 2. Obtenez la racine, intermédiaire (si applicableStep 5. et certificat d'application d'autorité de certification.

1. Fournissez les informations primaires et secondaires de la demande de signature de certificat de serveurs (CSR) à l'autorité de Certifcate de tiers comme Verisign, Thawte, GeoTrust etc.

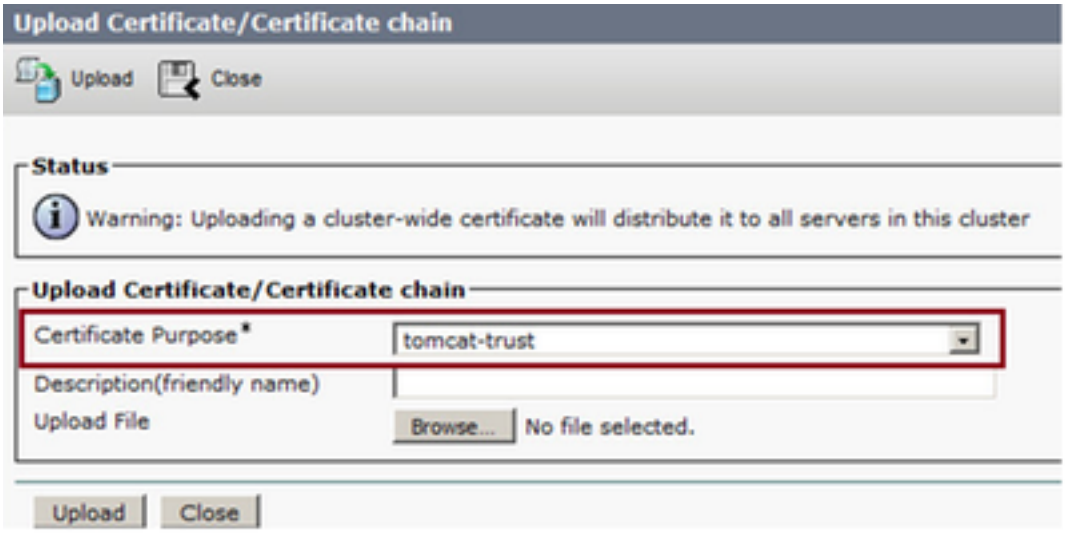
2. De l'autorité de certifcate on devrait recevoir la chaîne de certificat suivante pour les serveurs primaires et secondory.

- **Serveurs de finesse :** Certificat de racine, d'intermédiaire (facultative) et d'application
- **Serveurs CUIC :** Certificat de racine, d'intermédiaire (facultative) et d'application
- **Services vivants de données :** Certificat de racine, d'intermédiaire (facultative) et d'application

Étape 3. Certificats de téléchargement aux serveurs.

Cette section décrit sur la façon dont télécharger la chaîne de certificat correctement sur la finesse, CUIC et vivre des serveurs de données.

Serveurs de finesse

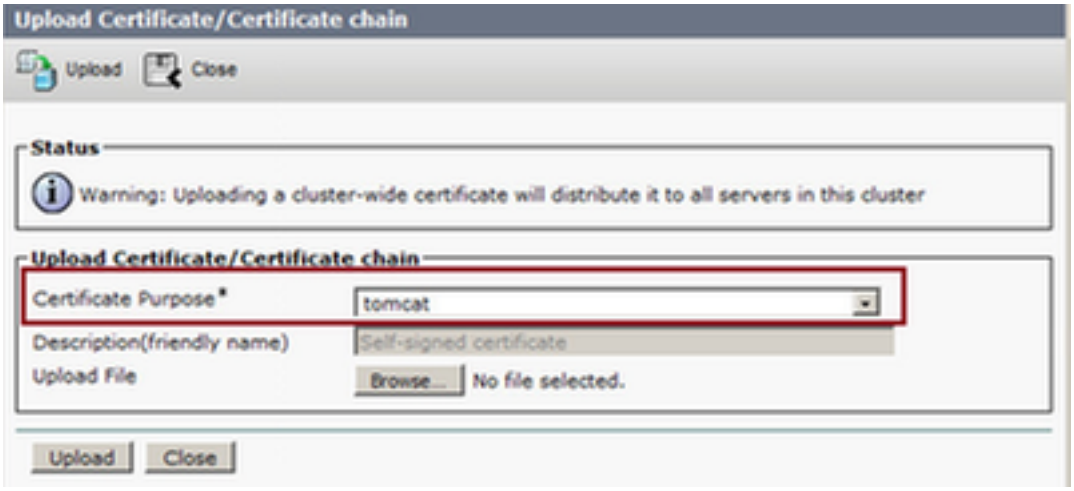


1. Téléchargez le certificat racine sur le serveur primaire de finesse avec l'aide de ces étapes :

   Étape 1. À la page du système d'exploitation de gestion de Cisco Unified Communications de serveur primaire, naviguez vers la **Gestion de Sécurité > de certificat > le certificat de téléchargement.**
   Étape 2. De la liste déroulante de nom de certificat, Tomcat-confiance choisie.
   Étape 3. Dans le champ File de téléchargement, le clic parcourent et parcourent au fichier de certificat racine.
   Étape 4. Cliquez sur Upload le fichier.

2. Téléchargez le certificat intermédiaire sur le serveur primaire de Fineese avec l'aide de ces étapes :

   Étape 1. Les étapes sur télécharger le certififcate intermédiaire correspond le certificat racine suivant les indications de l'étape 1.
   Étape 2. À la page du système d'exploitation de gestion de Cisco Unified Communications de serveur primaire, naviguez vers la **Gestion de Sécurité > de certificat > le certificat de téléchargement.**
   Étape 3. De la liste déroulante de nom de certificat, Tomcat-confiance choisie.
   Étape 4. Dans le champ File de téléchargement, le clic parcourent et parcourent au fichier du certificat intermédiaire.
   Étape 5. Cliquez sur Upload.Remarque: Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondaires elle n'est pas nécessaire pour télécharger la racine ou intermédiaire délivrez un certificat au serveur secondaire de finesse.
3. Téléchargez le certificat primaire de serveur d'application de finesse suivant les indications de l'image :



Étape 1. De la liste déroulante de nom de certificat, chat choisi.Étape 2. Dans le champ File de téléchargement, le clic **parcourent** et parcourent au fichier du certificat d'application.
Étape 3. Cliquez sur Upload pour télécharger le fichier.

4. Téléchargez le certificat secondaire de serveur d'application de Fineese.
   Dans cette étape suivez le même processus que mentionné dans l'étape 3 sur le serveur secondaire pour son propre certificat d'application.

5. Maintenant vous pouvez redémarrer les serveurs.
   Accédez au CLI sur les serveurs primaires et secondaires de finesse et entrez dans le **redémarrage du système d'utils de** commande pour redémarrer les serveurs.

Serveurs CUIC (n'assumant aucun Certificats d'intermédiaire actuel dans la chaîne de certificat)

1. Certificat racine de téléchargement sur le serveur primaire CUIC.

   Étape 1. À la page du système d'exploitation de gestion de Cisco Unified Communications de serveur primaire, naviguez **chaîne** vers la **Gestion de Sécurité > de certificat > de téléchargement certificat/certificat**.
   Étape 2. De la liste déroulante de nom de certificat, Tomcat-confiance choisie.
   Étape 3. Dans le champ File de téléchargement, le clic parcourent et parcourent au fichier de certificat racine.
   Étape 4. Cliquez sur Upload le fichier.Remarque: Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondaires elle n'est pas nécessaire pour télécharger le certificat racine au serveur secondaire CUIC.

2. Certificat primaire de serveur d'application du téléchargement CUIC.

   Étape 1. De la liste déroulante de nom de certificat, chat choisi.
   Étape 2. Dans le champ File de téléchargement, le clic parcourent et parcourent au fichier du certificat d'application.
   Étape 3. Cliquez sur Upload le fichier.
3. Certificat secondaire de serveur d'application du téléchargement CUIC.
   Suivez le même processus comme stipulé dans l'étape (2) sur le serveur secondaire pour son propre certificat d'application

4. Serveurs de reprise
   Accédez au CLI sur les serveurs primaires et secondaires CUIC et sélectionnez la commande **« redémarrage du système d'utils »** de redémarrer les serveurs.
   Remarque: Si l'autorité CA fournit la chaîne de certificat qui inclut les Certificats intermédiaires puis les étapes mentionnées dans les serveurs de finesse que la section s'appliquent aux services CUIC aussi bien.

Serveurs de données vivants

1. Les étapes impliquées sur des serveurs de Vivant-données pour télécharger les Certificats est identique à la finesse ou aux serveurs CUIC selon la chaîne de certificat.

2. Certificat racine de téléchargement sur le serveur primaire de Vivant-données.

   Étape 1. À la page du système d'exploitation de gestion de Cisco Unified Communications de serveur primaire, naviguez vers la **Gestion de Sécurité > de certificat > le certificat de téléchargement**.
   Étape 2. De la liste déroulante de nom de certificat, Tomcat-confiance choisie.
   Étape 3. Dans le champ File de téléchargement, le clic **parcourent** et parcourent au fichier de certificat racine.
   Étape 4. Cliquez sur Upload.

3. Certificat intermédiaire de téléchargement sur le serveur primaire de Vivant-données.

   Étape 1. Les étapes sur télécharger le certififcate intermédiaire correspond le certificat racine suivant les indications de l'étape 1.
   Étape 2. À la page du système d'exploitation de gestion de Cisco Unified Communications de serveur primaire, naviguez vers la **Gestion de Sécurité > de certificat > le certificat de téléchargement**.
   Étape 3. De la liste déroulante de nom de certificat, Tomcat-confiance choisie.
   Étape 4. Dans le champ File de téléchargement, le clic **parcourent** et parcourent au fichier du certificat intermédiaire.
   Étape 5. Cliquez sur Upload.
   Remarque: Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondaires elle n'est pas nécessaire pour télécharger la racine ou intermédiaire délivrez un certificat au serveur secondaire de Vivant-données.
4. Certificat primaire de serveur d'application de Vivant-données de téléchargement**.**

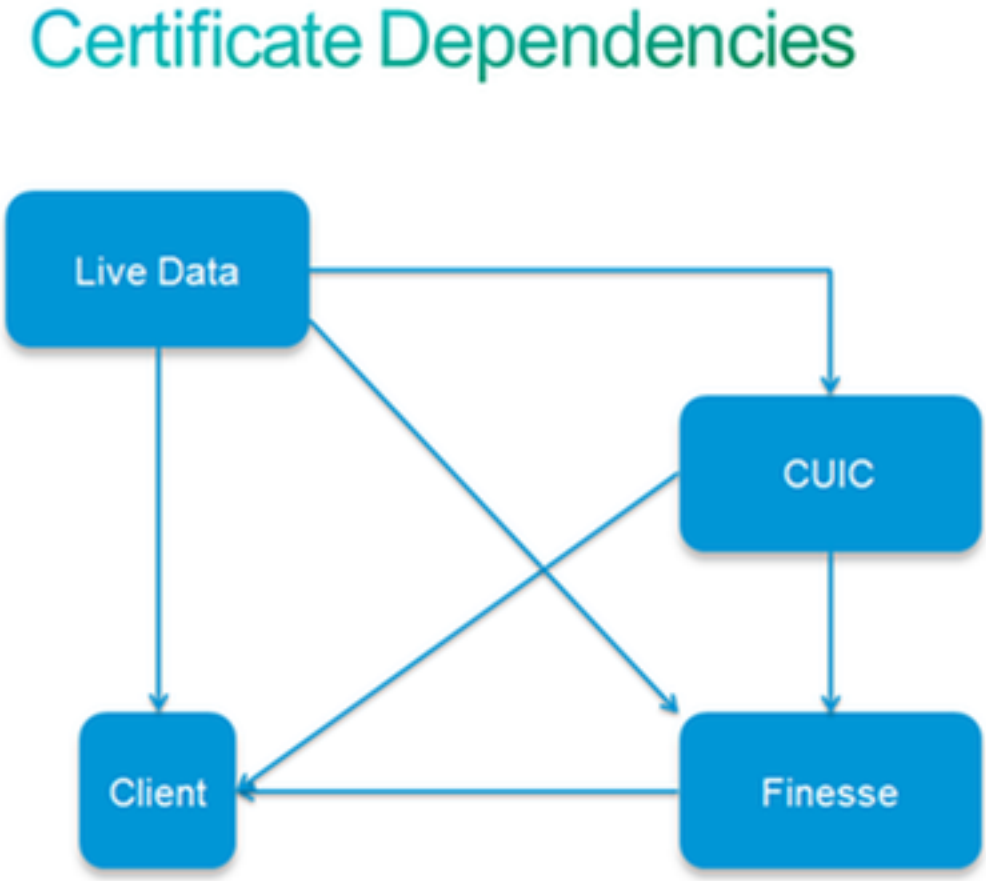
   Étape 1. De la liste déroulante de nom de certificat, chat choisi.
   Étape 2. Dans le champ File de téléchargement, le clic **parcourent** et parcourent au fichier du certificat d'application.
   Étape 3. Cliquez sur Upload.

5. Certificat secondaire de serveur d'application de Vivant-données de téléchargement.
   Suivez les mêmes étapes que mentionnées ci-dessus dans (4) sur le serveur secondory pour son propre certificat d'application.

6. Serveurs de reprise
   Accédez au CLI sur les serveurs primaires et secondaires de finesse et sélectionnez la commande **« redémarrage du système d'utils »** de redémarrer les serveurs.

Dépendances vivantes de certificat de serveurs de données

En tant que serveurs de données vivants interagissez avec CUIC et serveurs de finesse, là sont des dépendances de certificat entre ces serveurs suivant les indications de l'image :



En vue de la chaîne de certificat de CA de tiers les Certificats de racine et d'intermédiaire sont mêmes pour tous les serveurs dans l'organisation. En conséquence pour que le serveur de données Live fonctionne correctement, vous devez s'assurer que la finesse et les serveurs CUIC ont les Certificats de racine et d'intermédiaire correctement chargés dans là des conteneurs de Tomcat-confiance.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.