Soluzione Unified CCE: procedura per ottenere e caricare certificati CA di terze parti (versione 11.x)

Sommario

Introduzione

Lo scopo di questo documento è spiegare in dettaglio le procedure necessarie per ottenere e installare un certificato di un'Autorità di certificazione (CA), generato da un fornitore di terze parti per stabilire una connessione HTTPS tra i server Finesse, Cisco Unified Intelligence Center (CUIC) e Live Data (LD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Contact Center Enterprise (UCCE)
- Cisco Live Data (LD)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Finesse

- Certificato CA

Componenti usati

Le informazioni utilizzate nel documento si basano sulla versione 11.0(1) della soluzione UCCE.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, verificare di aver compreso l'impatto potenziale di qualsiasi passaggio.

Premesse

Per utilizzare HTTPS per una comunicazione sicura tra i server Finesse, CUIC e Live Data, è necessario configurare i certificati di protezione. Per impostazione predefinita, questi server forniscono certificati autofirmati che vengono utilizzati per consentire ai clienti di acquistare e installare certificati firmati da CA (Certification Authority). Questi certificati CA possono essere ottenuti da un fornitore di terze parti come VeriSign, Thawte, GeoTrust o possono essere prodotti internamente.

Configurazione

La configurazione del certificato per la comunicazione HTTPS nei server Finesse, CUIC e Live Data richiede i seguenti passaggi:

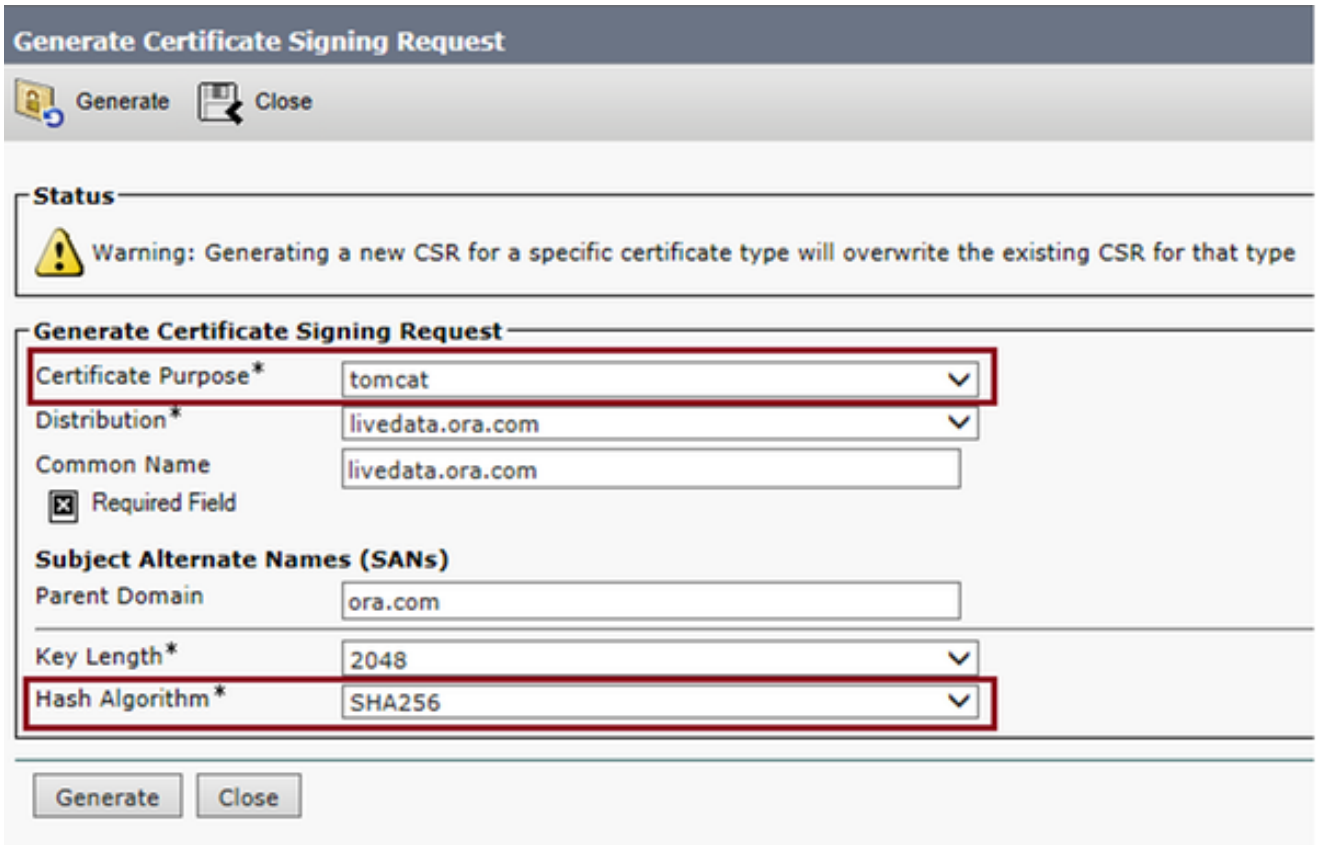
1. Generare e scaricare la richiesta di firma del certificato (CSR).
2. Ottenere il certificato radice, intermedio (se applicabile) e di applicazione dall'autorità di certificazione utilizzando CSR.
3. Caricare i certificati nei server.

Passaggio 1. Generare e scaricare la richiesta di firma del certificato (CSR).

1. La procedura descritta per la generazione e il download di CSR è la stessa per i server dati Finesse, CUIC e Live.

2. Aprire la pagina Cisco Unified Communications Operating System Administration (Amministrazione del sistema operativo di Cisco Unified Communications) utilizzando l'URL indicato e accedere con l'account di amministratore del sistema operativo creato durante il processo di installazione
   https://FQDN:8443/cmplatform

3. Generare la richiesta di firma del certificato (CSR) come illustrato nell'immagine:



Passaggio 1. Passare a Protezione > Gestione certificati > Genera CSR.

Passaggio 2. Dall'elenco a discesa Nome scopo certificato selezionare tomcat.

Passaggio 3. Selezionare Algoritmo hash e lunghezza chiave a seconda delle esigenze aziendali.

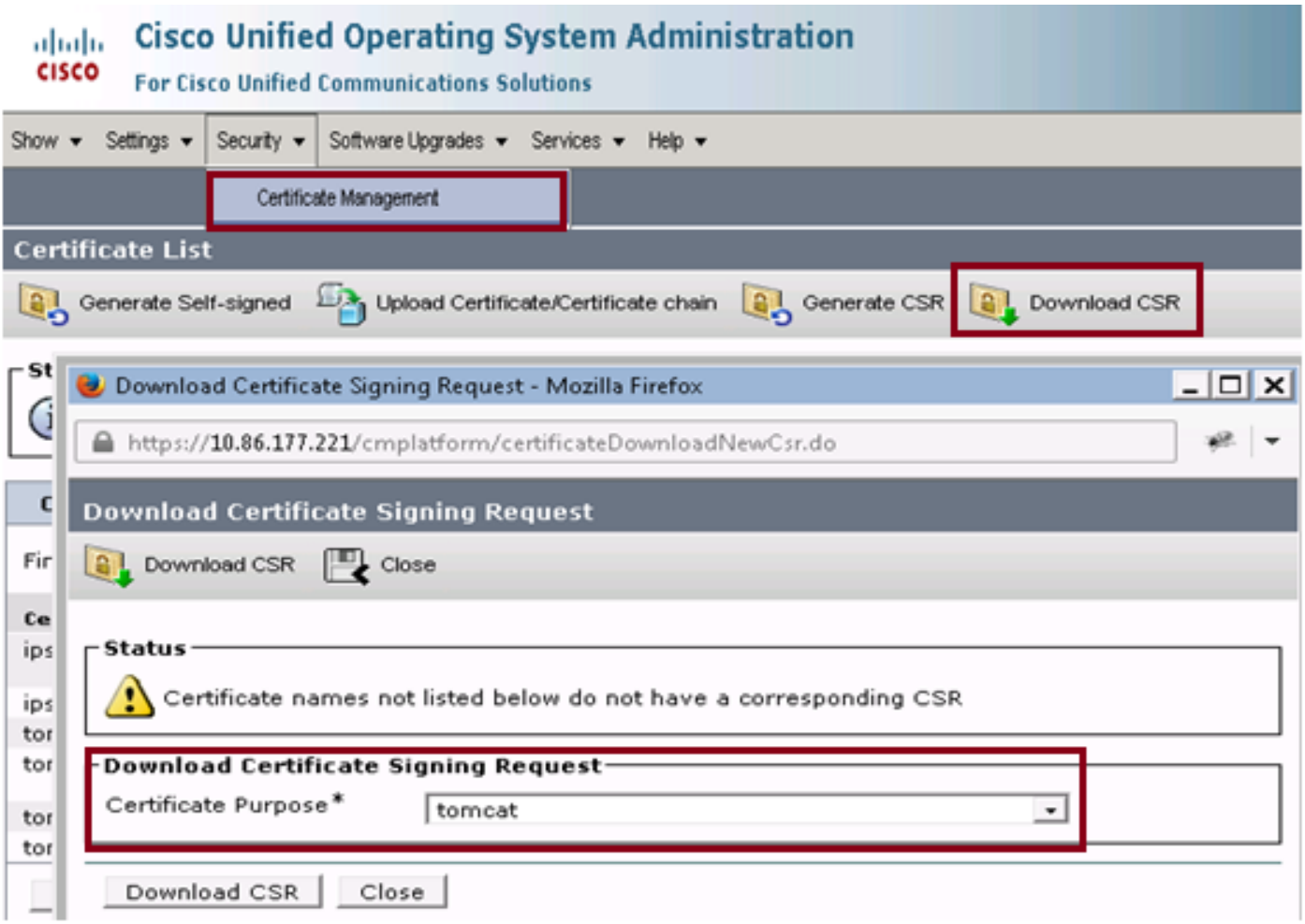
- Lunghezza chiave: 2048 \ Algoritmo hash: si consiglia SHA256

Passaggio 4. Fare clic su Genera CSR.

Nota: se l'azienda richiede che il campo del dominio padre relativo ai nomi soggetto alternativi (SAN) sia compilato con il nome di dominio, tenere presente gli indirizzi dei problemi indicati nel documento "Rilascio di SAN con certificato firmato da terze parti in Finesse".

---

4. Scaricare la richiesta di firma del certificato (CSR) come illustrato nell'immagine:



Passaggio 1. Selezionare Protezione > Gestione certificati > Scarica CSR.
Passaggio 2. Dall'elenco a discesa Nome certificato selezionare tomcat.
Passaggio 3. Fare clic su Download CSR.

Nota:

Nota: eseguire la procedura sopra descritta nel server secondario utilizzando l'URL https://FQDN:8443/cmplatform per ottenere i CSR per Certificate Authority

---

Passaggio 2. Ottenere il certificato radice, intermedio (se applicabile)Fase 5. e applicazione da Certificate Authority.

1. Fornire le informazioni CSR (Certificate Signing Request) del server primario e secondario ad autorità di certificazione di terze parti quali VeriSign, Thawte, GeoTrust e così via.

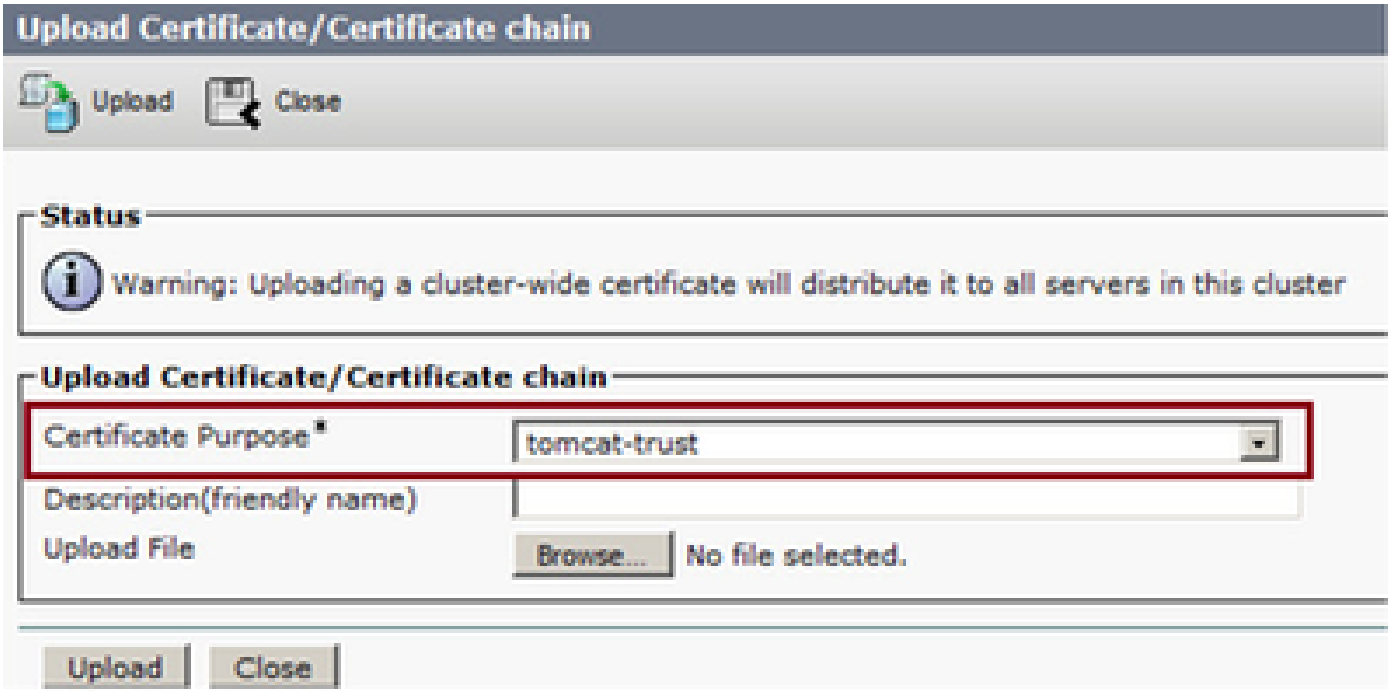
2. Dall'autorità di certificazione si dovrebbe ricevere la seguente catena di certificati per i server principale e secondario.

- Server Finesse: radice, intermedio (facoltativo) e certificato applicazione
- Server CUIC: radice, intermedio (facoltativo) e certificato applicazione
- Server di dati attivi: radice, intermedio (facoltativo) e certificato applicazione

Passaggio 3. Caricare i certificati nei server.

In questa sezione viene descritto come caricare correttamente la catena di certificati nei server dati Finesse, CUIC e Live.

Server Finesse



1. Caricare il certificato radice sul server Finesse primario con la seguente procedura:

   Passaggio 1. Nella pagina Amministrazione del sistema operativo Cisco Unified Communications del server principale passare a Protezione > Gestione certificati > Carica certificato.
   Passaggio 2. Dall'elenco a discesa Nome certificato selezionare tomcat-trust.
   Passaggio 3. Nel campo Carica file fare clic su Sfoglia e individuare il file del certificato radice.
   Passaggio 4. Fare clic su Carica file.

2. Caricare il certificato intermedio sul server Fineese primario eseguendo la procedura seguente:

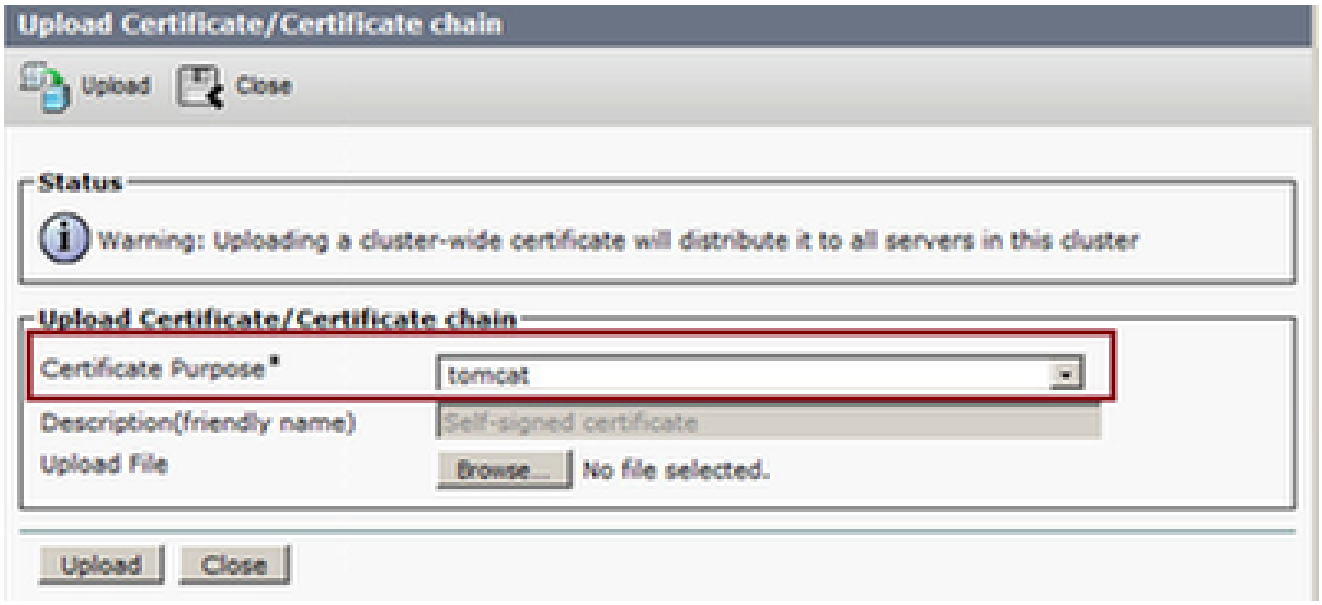
   Passaggio 1. La procedura per il caricamento del certificato intermedio è uguale a quella del certificato radice, come illustrato al passaggio 1.
   Passaggio 2. Nella pagina Amministrazione del sistema operativo Cisco Unified Communications del server principale, selezionare Sicurezza > Gestione certificati > Carica certificato.
   Passaggio 3. Dall'elenco a discesa Nome certificato selezionare tomcat-trust.

Passaggio 4. Nel campo Carica file, fare clic su Sfoglia e selezionare il file del certificato intermedio.
Passaggio 5. Fare clic su Upload.

Nota: poiché l'archivio Tomcat-trust viene replicato tra i server primario e secondario, non è necessario caricare il certificato radice o intermedio sul server finesse secondario.

---

3. Caricare il certificato dell'applicazione server Finesse primario come mostrato nell'immagine:



Passaggio 1. Dall'elenco a discesa Nome certificato selezionare tomcat.

Passaggio 2. Nel campo Carica file fare clic su Sfoglia e individuare il file del certificato dell'applicazione.
Passaggio 3. Fare clic su Upload per caricare il file.

4. Caricare il certificato dell'applicazione server Fineese secondario.

In questo passaggio fSeguire la stessa procedura indicata al passaggio 3 sul server secondario per il proprio certificato applicazione.

5. Ora è possibile riavviare i server.
Accedere alla CLI sui server Finesse primario e secondario e immettere il comando utilizza il riavvio del sistema per riavviare i server.

Server CUIC (presumendo che non siano presenti certificati intermedi nella catena di certificati)

1. Carica certificato radice nel server CUIC primario.

Passaggio 1. Nella pagina Amministrazione del sistema operativo Cisco Unified Communications del server principale passare a Protezione > Gestione certificati > Carica catena di certificati/certificati.
Passaggio 2. Dall'elenco a discesa Nome certificato selezionare tomcat-trust.
Passaggio 3. Nel campo Carica file fare clic su Sfoglia e individuare il file del certificato radice.
Passaggio 4. Fare clic su Carica file.

Nota: poiché l'archivio di attendibilità tomcat viene replicato tra i server primario e secondario, non è necessario caricare il certificato radice nel server CUIC secondario.

---

2. Carica il certificato dell'applicazione server CUIC primaria.

Passaggio 1. Dall'elenco a discesa Nome certificato selezionare tomcat.
Passaggio 2. Nel campo Carica file fare clic su Sfoglia e individuare il file del certificato dell'applicazione.
Passaggio 3. Fare clic su Carica file.

3. Carica il certificato dell'applicazione server CUIC secondaria.
Seguire la stessa procedura indicata al passaggio 2 sul server secondario per il proprio certificato applicazione

4. Riavvia server
Accedere alla CLI sui server CUIC primario e secondario e immettere il comando "utils system restart" per riavviare i server.

Nota: se l'autorità CA fornisce la catena di certificati che include i certificati intermedi, i passi indicati nella sezione Server Finesse sono applicabili anche ai server CUIC.

Server Live Data

1. I passaggi necessari per caricare i certificati nei server Live-Data sono identici ai server Finesse o CUIC, a seconda della catena di certificati.

2. Carica il certificato radice nel server Live-Data primario.

Passaggio 1. Nella pagina Amministrazione del sistema operativo Cisco Unified Communications del server principale, selezionare Sicurezza > Gestione certificati > Carica certificato.
Passaggio 2. Dall'elenco a discesa Nome certificato selezionare tomcat-trust.
Passaggio 3. Nel campo Carica file, fare clic su sfoglia per individuare il file del certificato radice.

Passaggio 4. Fare clic su Upload.

3. Carica il certificato intermedio sul server Live-Data primario.

   Passaggio 1. La procedura per il caricamento del certificato intermedio è uguale a quella del certificato radice, come illustrato al passaggio 1.
   Passaggio 2. Nella pagina Amministrazione del sistema operativo Cisco Unified Communications del server principale, selezionare Sicurezza > Gestione certificati > Carica certificato.
   Passaggio 3. Dall'elenco a discesa Nome certificato selezionare tomcat-trust.
   Passaggio 4. Nel campo Carica file, fare clic su sfoglia e selezionare il file del certificato intermedio.
   Passaggio 5. Fare clic su Upload.

   > Nota: poiché l'archivio Tomcat-trust viene replicato tra i server primario e secondario, non è necessario caricare il certificato radice o intermedio nel server secondario Live-Data.

   ---

4. Carica certificato applicazione server Live-Data primario.

   Passaggio 1. Dall'elenco a discesa Nome certificato selezionare tomcat.
   Passaggio 2. Nel campo Carica file fare clic su Sfoglia e individuare il file del certificato dell'applicazione.
   Passaggio 3. Fare clic su Upload.

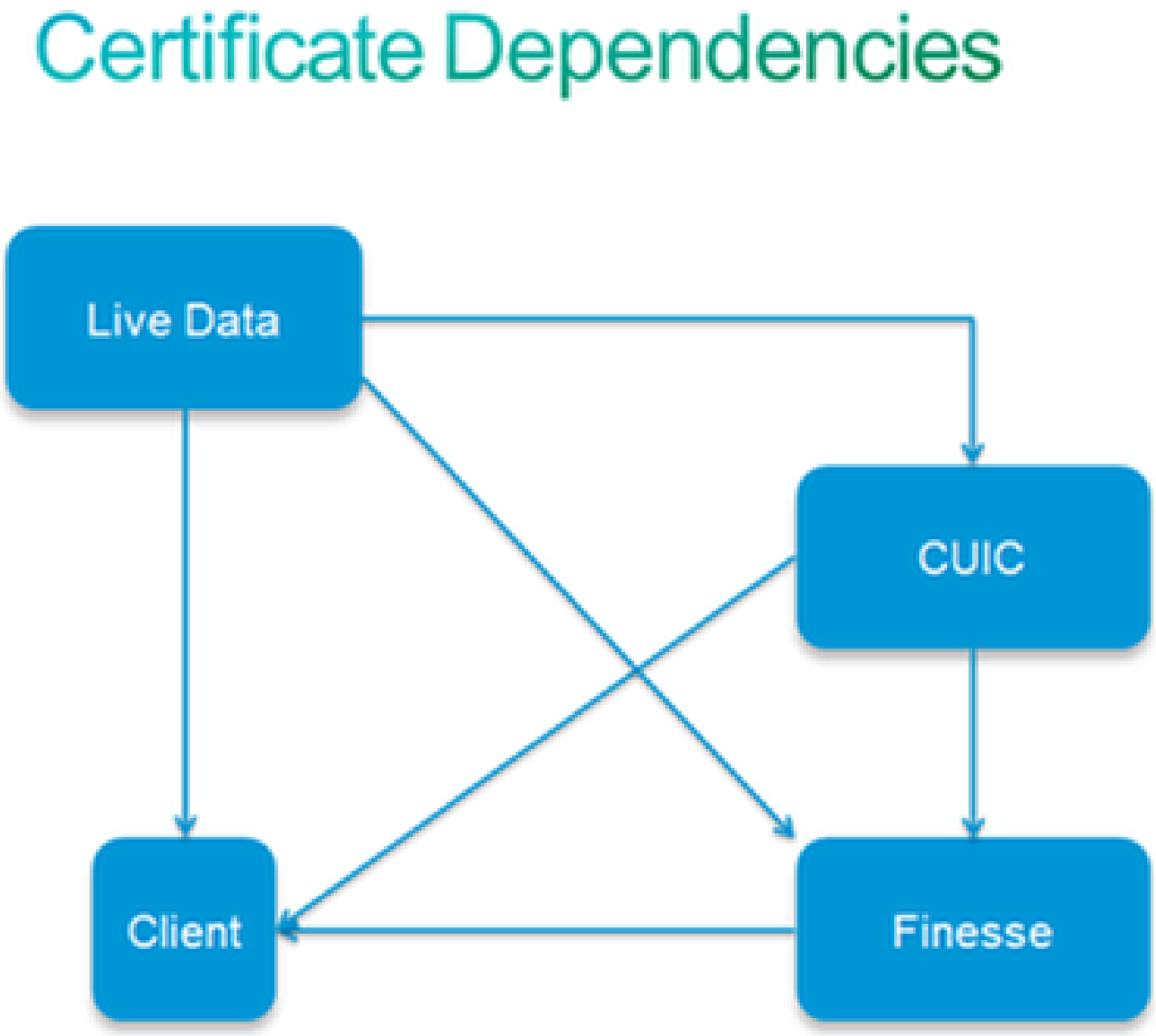
5. Carica il certificato secondario dell'applicazione server Live Data.

   Eseguire la stessa procedura descritta in (4) sul server secondario per il proprio certificato applicazione.

6. Riavvia server
   Accedere alla CLI sui server Finesse primario e secondario e immettere il comando "utils system restart" per riavviare i server.

Dipendenze dei certificati dei server Live Data

Poiché i server di dati in tempo reale interagiscono con i server CUIC e Finesse, esistono dipendenze di certificato tra questi server, come mostrato nell'immagine:



Per quanto riguarda la catena di certificati CA di terze parti, i certificati radice e intermedio sono gli stessi per tutti i server dell'organizzazione. Di conseguenza, affinché il server Live Data funzioni correttamente, è necessario verificare che i server Finesse e CUIC dispongano dei certificati radice e intermedi correttamente caricati nei contenitori Tomcat-Trust.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).