Унифицированное Решение для CCE: Процедура, чтобы Получить и Загрузить Сторонние сертификаты CA (Версия 11. x

Содержание

Введение

Этот документ стремится объяснять подробно шаги, включенные, чтобы получить и установить сертификат Центра сертификации (CA), генерируемый от стороннего поставщика для установления Подключения HTTPS между Изяществом, Cisco Unified Intelligence Center (CUIC) и серверами Оперативных данных (LD).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco Unified Contact Center Enterprise (UCCE)
- Данные Cisco live (LD)
- Cisco Unified Intelligence Center (CUIC)
- Изящество Cisco
- CA сертифицируемый

Используемые компоненты

Информация, используемая в документе, основывается на версии решения 11.0 (1) UCCE.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, удостоверьтесь, что вы понимаете потенциальное воздействие любого шага.

Общие сведения

Для использования HTTPS для безопасной связи между Изяществом, CUIC и Оперативными Серверами данных, настройка сертификатов безопасности необходима. По умолчанию эти серверы предоставляют самоподписанные certifcates, которые используются, или клиенты могут обеспечить и установить подписанные сертификаты Центра сертификации (CA). Они CA certs могут быть получены или от стороннего поставщика как VeriSign, Thawte, GeoTrust или могут быть произведены внутренне.

Настройка

Устанавливая сертификат для Связи HTTPS в Изяществе, CUIC и Оперативные Серверы данных требуют этих шагов:

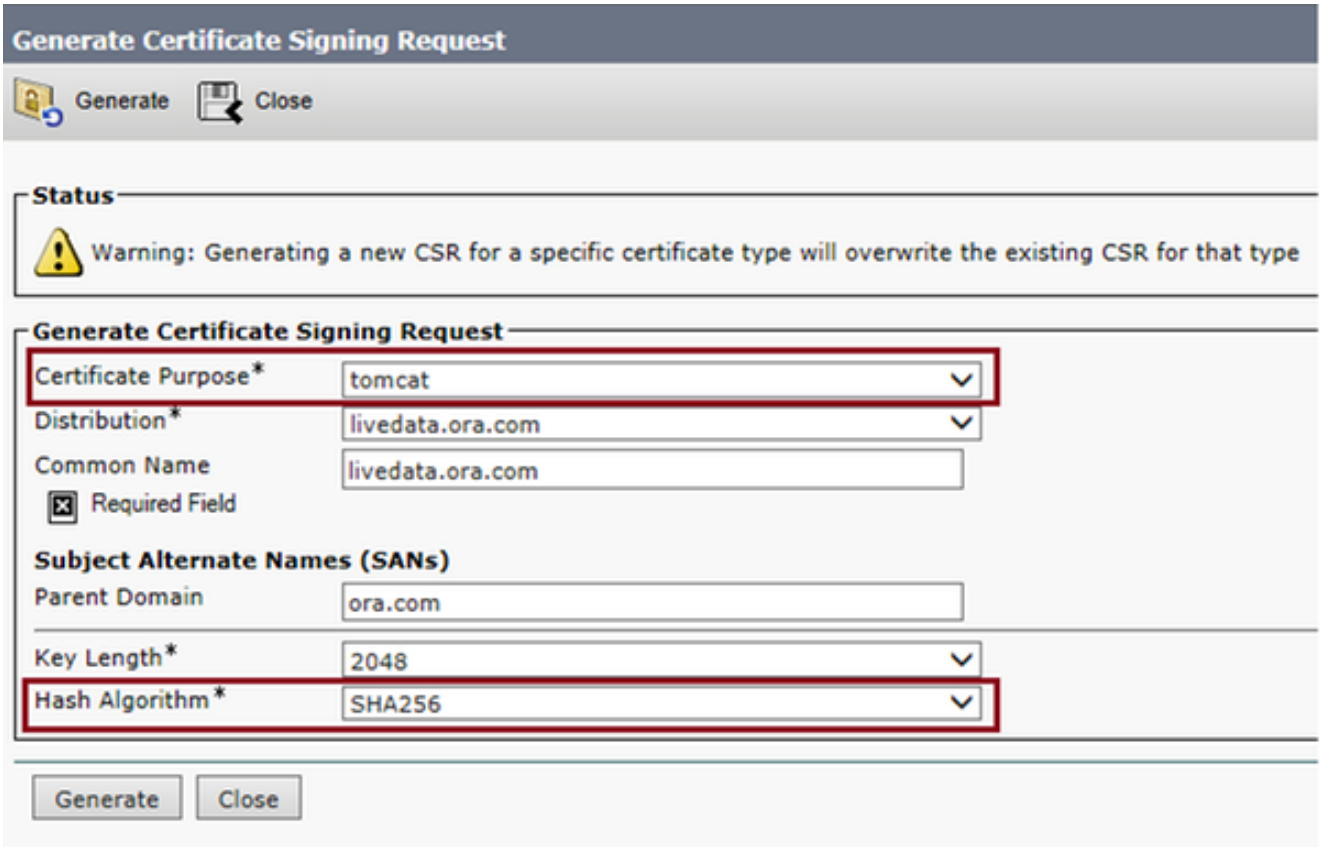
1. Генерируйте и загрузите Запрос подписи сертификата (CSR).
2. Получите Root, промежуточное звено (если применимо) и сертификат приложения от Центра сертификации с помощью CSR.
3. Сертификаты загрузки к серверам.

Шаг 1. Генерируйте и загрузите Запрос подписи сертификата (CSR).

1. Шаги, описанные здесь для генерации и загрузки CSR, являются тем же для Изящества, CUIC и Оперативные данные разъединяют.

2. Откройте **Страницу администратора Операционной системы Унифицированной связи Cisco** с помощью установленного URL и регистрируйтесь с учетной записью администратора ОС, созданной во время процесса установки **https://FQDN:8443/cmplatform**

3. Генерируйте Запрос подписи сертификата (CSR) как показано в образе:

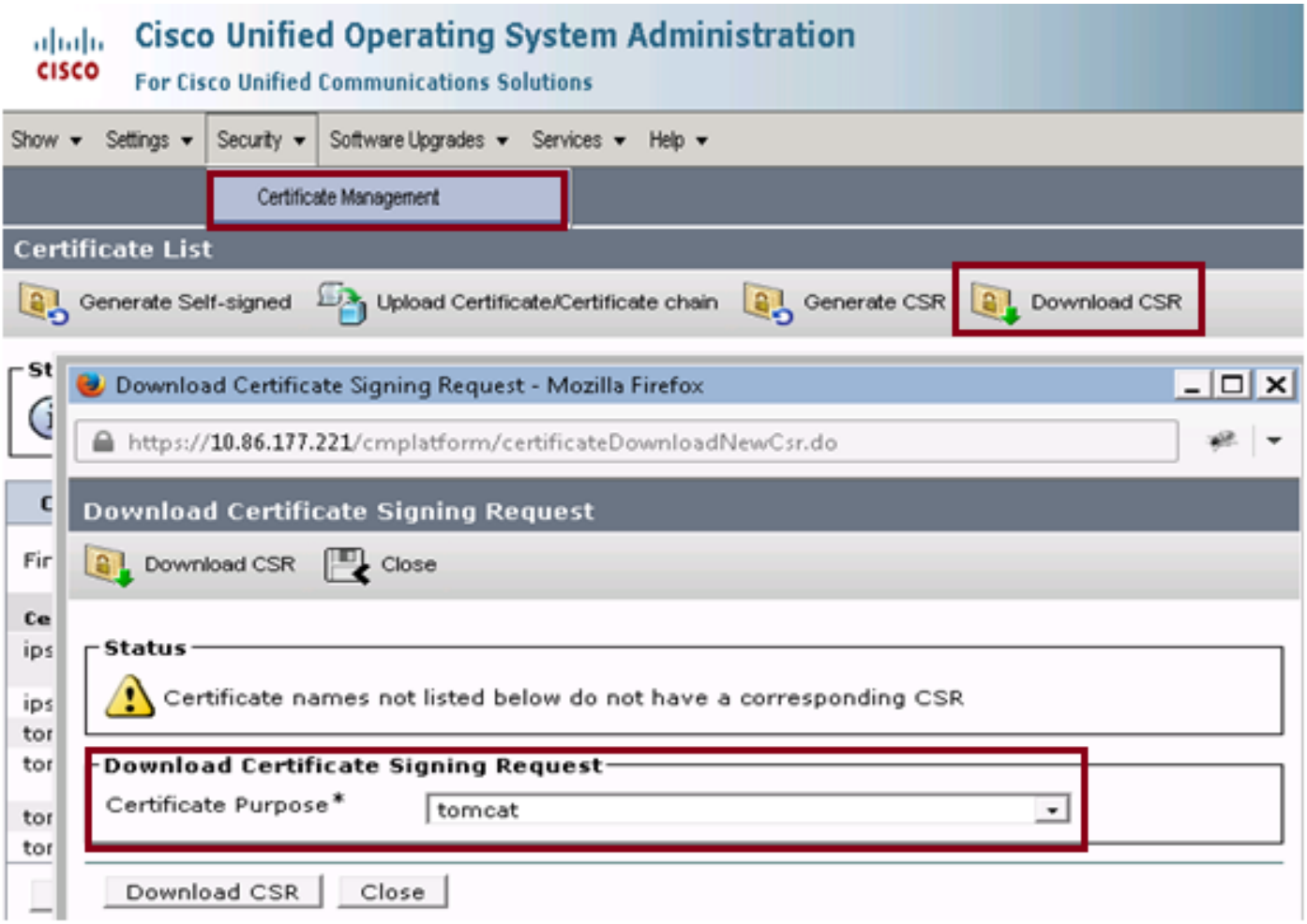


Шаг 1. Перейдите к **Безопасности> Управление сертификатами>, Генерируют CSR**.Шаг 2. От выпадающего списка Названия Цели Сертификата выберите tomcat.Шаг 3. Выберите Hash Algorithm и длину ключа depeding на потребности организации.

- Длина ключа: 2048 \Алгоритм хэширования: SHA256 рекомендуется

Шаг 4. . Нажмите **Generate CSR**.**Примечание:** Если бизнес требует Подчиненных Альтернативных названий (SANs), родительское поле domain, чтобы быть заполненным доменным именем тогда знает об адресах проблемы в документе "проблема SANs с Подписанным сертификатом Третьей стороны в Изяществе".

4. Загрузите Запрос подписи сертификата (CSR) как показано в образе:



Шаг 1. Перейдите к **Безопасности> Управление сертификатами> CSR Загрузки**.
Шаг 2. От выпадающего списка Названия Сертификата выберите tomcat.
Шаг 3. Нажмите **Download CSR**.

Примечание:

> **Примечание:** Выполните вышеупомянутые шаги в использование дополнительного сервера URL **https://FQDN:8443/cmplatform** для получения CSR для Центра сертификации

Шаг 2. Получите Root, Промежуточное звено (если applicableStep 5. и сертификат Приложения от Центра сертификации.

1. Предоставьте основного и информацию о Запросе подписи сертификата (CSR) дополнительных серверов к полномочиям третьей стороны Сертифкэйт как VeriSign, Thawte, GeoTrust и т.д.

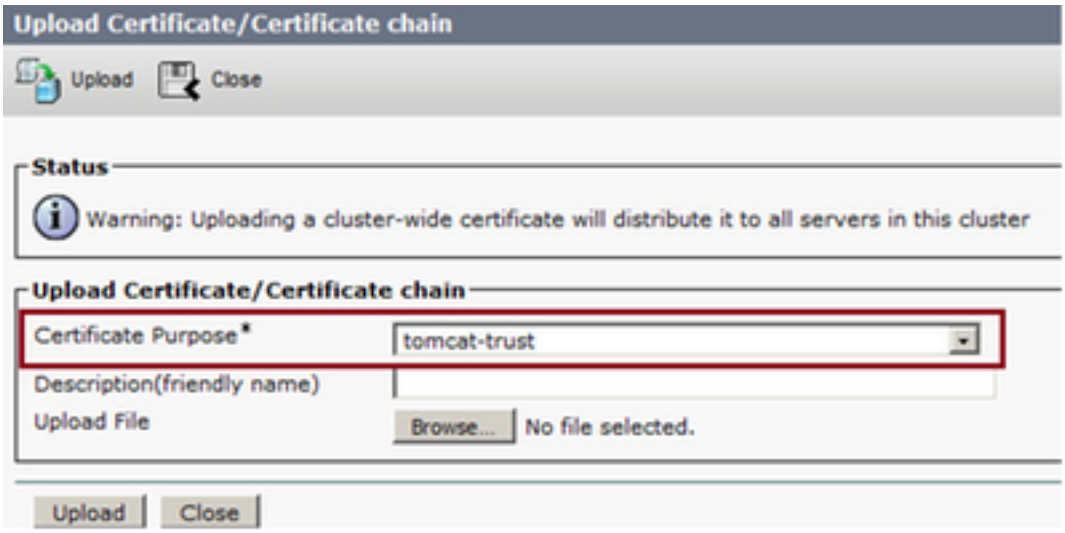
2. От certifcate полномочий нужно получить следующую цепочку сертификатов для основных и secondory серверов.

- **Серверы изящества:** Root, (дополнительное) Промежуточное звено и сертификат Приложения
- **Серверы CUIC:** Root, (дополнительное) Промежуточное звено и сертификат Приложения
- **Оперативные подачи данных:** Root, (дополнительное) Промежуточное звено и сертификат Приложения

Шаг 3. Сертификаты загрузки к серверам.

В этом разделе описываются о том, как загрузить цепочку сертификатов правильно на Изяществе, CUIC и Оперативных серверах данных.

Серверы изящества

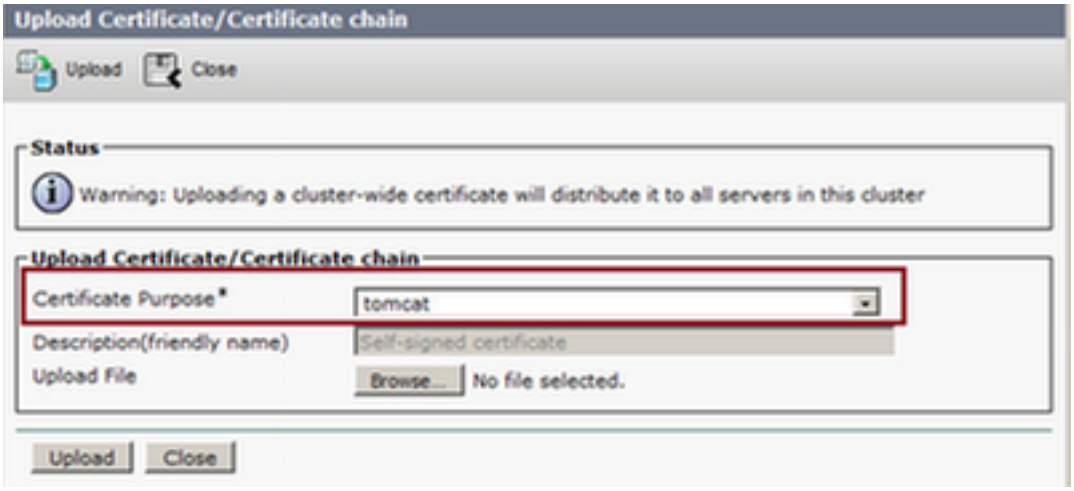


1. Загрузите Корневой сертификат на Основном сервере Изящества с помощью этих шагов:

   Шаг 1. На основном сервере Страница администратора Операционной системы Унифицированной связи Cisco перейдите к **Безопасности> Управление сертификатами> Сертификат Загрузки.**
   Шаг 2. От выпадающего списка Названия Сертификата выберите доверие tomcat.
   Шаг 3. В Поле файла Загрузки щелчок просматривает и переходит к файлу корневого сертификата.
   Шаг 4. . Щелкните Upload File (Загрузить файл).

2. Загрузите промежуточный сертификат на Основном сервере Fineese с помощью этих шагов:

   Шаг 1. Шаги в загрузку certififcate промежуточного звена являются тем же как корневой сертификат как показано в шаге 1.
   Шаг 2. На основном сервере Страница администратора Операционной системы Унифицированной связи Cisco перейдите к **Безопасности> Управление сертификатами> Сертификат Загрузки.**
   Шаг 3. От выпадающего списка Названия Сертификата выберите доверие tomcat.
   Шаг 4. . В Поле файла Загрузки щелчок просматривает и переходит к Промежуточному файлу сертификата.
   Шаг 5. . Нажмите **Upload**.**Примечание:** Поскольку база доверенных сертификатов Tomcat реплицирована между основным и дополнительными серверами, не необходимо загрузить корневой или Промежуточный сертификат к вторичному серверу изящества.
3. Загрузите Основной сертификат серверного приложения Изящества как показано в образе:



Шаг 1. От выпадающего списка Названия Сертификата выберите tomcat.Шаг 2. В Поле файла Загрузки нажмите **Browse** и перейдите к файлу сертификата приложения.
Шаг 3. Нажмите **Upload** для загрузки файла.

4. Загрузите Вторичный сертификат серверного приложения Fineese.
   В этом шаге придерживаются того же процесса, как упомянуто в Шаге 3 в дополнительный сервер для его собственного сертификата приложения.

5. Теперь можно перезапустить серверы.
   Обратитесь к CLI на основных и вторичных серверах Изящества и введите **команду utils system restart** для перезапуска серверов.

Серверы CUIC (Принимающий промежуточные сертификаты представляют в цепочке сертификатов),

1. Корневой сертификат загрузки на основном сервере CUIC.

   Шаг 1. На основном сервере Страница администратора Операционной системы Унифицированной связи Cisco перейдите к **Безопасности> Управление сертификатами> Сертификат/Цепочка сертификатов Загрузки.**
   Шаг 2. От выпадающего списка Названия Сертификата выберите доверие tomcat.
   Шаг 3. В Поле файла Загрузки щелчок просматривает и переходит к файлу корневого сертификата.
   Шаг 4. . Щелкните Upload File (Загрузить файл).**Примечание:** Поскольку база доверенных сертификатов tomcat реплицирована между основным и дополнительными серверами, не необходимо загрузить корневой сертификат к Вторичному серверу CUIC.

2. Загрузите основной сертификат серверного приложения CUIC.

   Шаг 1. От выпадающего списка Названия Сертификата выберите tomcat.
   Шаг 2. В Поле файла Загрузки нажмите Browse и перейдите к файлу сертификата приложения.
   Шаг 3. Щелкните Upload File (Загрузить файл).
3. Загрузите вторичный сертификат серверного приложения CUIC.

Придерживайтесь того же процесса, как сообщили в шаге (2) в дополнительный сервер для его собственного сертификата приложения

4. Серверы перезапуска
   Обратитесь к CLI на основных и вторичных серверах CUIC и введите команду **"перезапуск системы utils"** для перезапуска серверов.
   Примечание: Если полномочия CA предоставляют цепочку сертификатов, которая включает промежуточные сертификаты тогда, шаги, упомянутые в разделе Серверов Изящества, применимы к подачам CUIC также.

Оперативные серверы данных

1. Шаги, включенные на Оперативных Серверах данных для загрузки сертификатов, идентичны Изяществу или серверам CUIC в зависимости от цепочки сертификатов.

2. Корневой сертификат загрузки на Основном Оперативном Сервере данных.

   Шаг 1. На основном сервере Страница администратора Операционной системы Унифицированной связи Cisco перейдите к **Безопасности> Управление сертификатами> Сертификат Загрузки**.
   Шаг 2. От выпадающего списка Названия Сертификата выберите доверие tomcat.
   Шаг 3. В Поле файла Загрузки щелчок **просматривает** и переходит к файлу корневого сертификата.
   Шаг 4. . Нажмите **Upload**.

3. Промежуточный сертификат загрузки на Основном Оперативном Сервере данных.

   Шаг 1. Шаги в загрузку certififcate промежуточного звена являются тем же как корневой сертификат как показано в шаге 1.
   Шаг 2. На основном сервере Страница администратора Операционной системы Унифицированной связи Cisco перейдите к **Безопасности> Управление сертификатами> Сертификат Загрузки**.
   Шаг 3. От выпадающего списка Названия Сертификата выберите доверие tomcat.
   Шаг 4. . В Поле файла Загрузки щелчок **просматривает** и переходит к Промежуточному файлу сертификата.
   Шаг 5. . Нажмите **Upload**.
   Примечание: Поскольку база доверенных сертификатов Tomcat реплицирована между основным и дополнительными серверами, не необходимо загрузить корневой или Промежуточный сертификат к Вторичному Оперативному Серверу данных.
4. Загрузите Основной сертификат приложения Оперативного Сервера данных**.**

   Шаг 1. От выпадающего списка Названия Сертификата выберите tomcat.
   Шаг 2. В Поле файла Загрузки нажмите **Browse** и перейдите к файлу сертификата приложения.
   Шаг 3. Нажмите **Upload**.

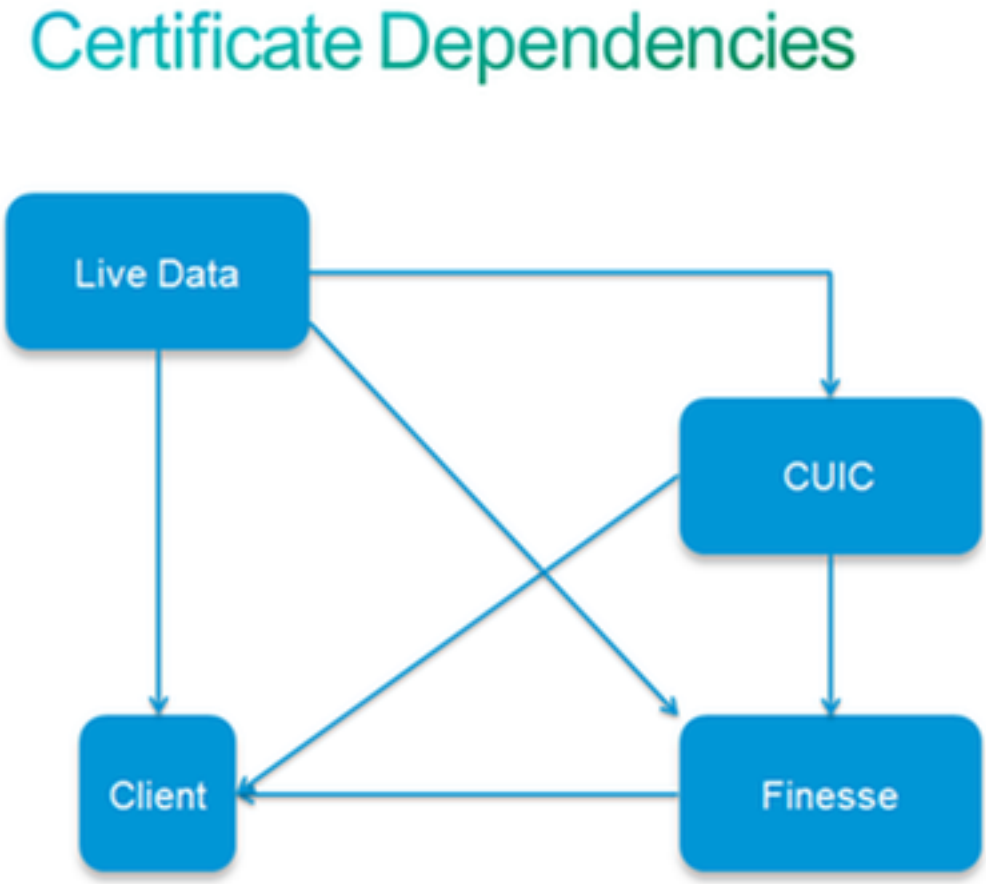
5. Загрузите Вторичный сертификат приложения Оперативного Сервера данных.

Выполните те же действия, как упомянуто выше в (4) на secondory сервере для его собственного сертификата приложения.

6. Серверы перезапуска
   Обратитесь к CLI на основных и вторичных серверах Изящества и введите команду **"перезапуск системы utils"** для перезапуска серверов.

Оперативные зависимости от сертификата серверов данных

Поскольку оперативные серверы данных взаимодействуют с CUIC и серверами Изящества, существуют зависимости от сертификата между этими серверами как показано в образе:



В отношении третьей стороны сертификат CA объединяет Корневые и Промежуточные сертификаты в цепочку, то же для всех серверов в организации. В результате для Оперативного сервера данных для работы должным образом необходимо гарантировать, что Изящество и серверы CUIC имеют Корневые и промежуточные сертификаты, должным образом загруженные в там Трастовых Tomcat контейнерах.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.