Implementieren der Wiederverwendung des Multi-SAN-Tomcat-Zertifikats für CallManager

Inhalt

Einleitung

In diesem Dokument wird ein schrittweiser Prozess zur Wiederverwendung des Multi-SAN Tomcat-Zertifikats für CallManager auf dem CUCM beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Unified Communications Manager (CUCM)
- CUCM-Zertifikate
- Identity Trust List (ITL)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- CUCM-Version 15 SU1

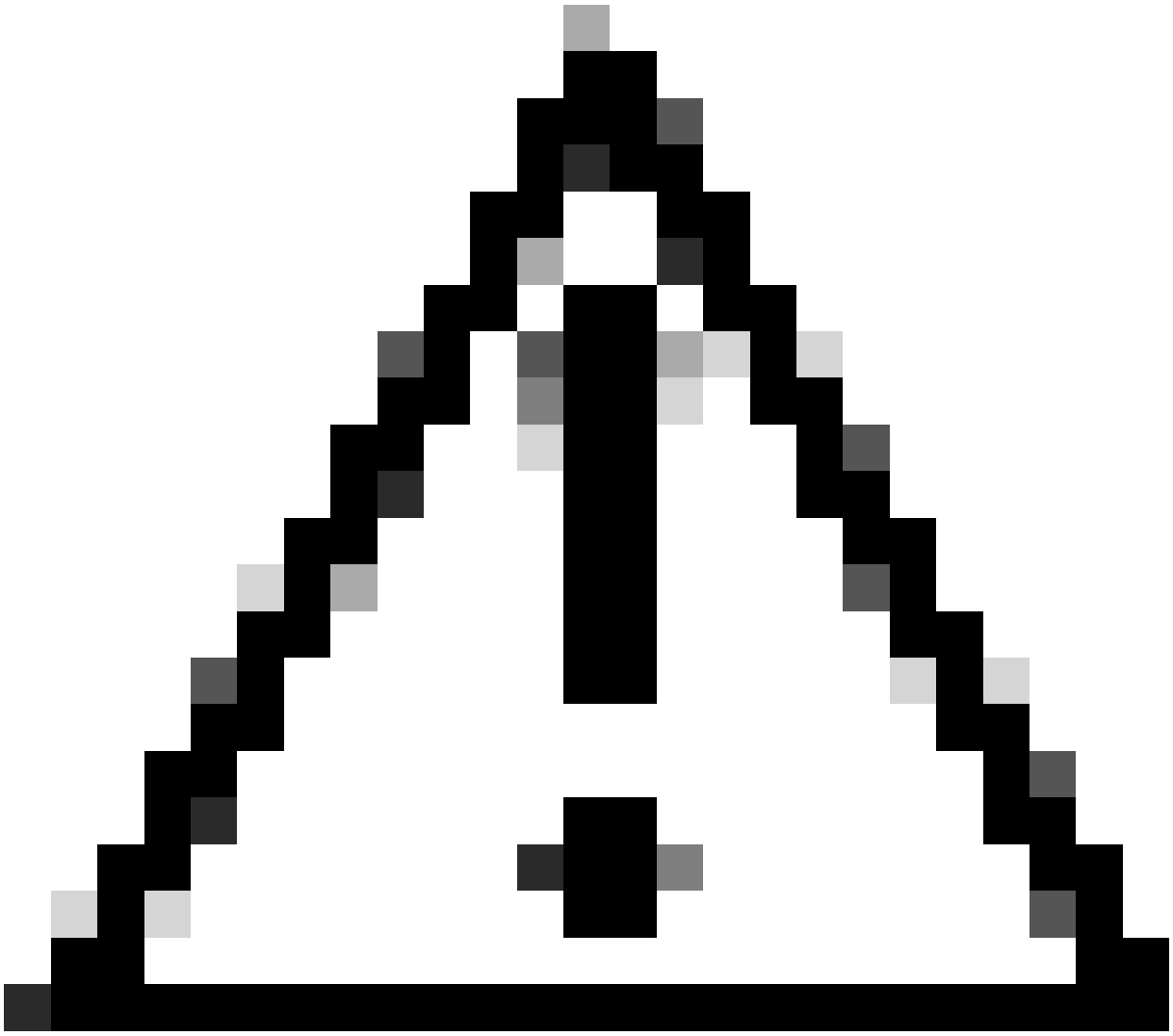
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In früheren Versionen von CUCM wurden für jeden Dienst unterschiedliche Zertifikate für den gesamten Cluster verwendet, wodurch sich die Anzahl der Zertifikate und die Kosten erhöhten. Dazu gehören Cisco Tomcat und Cisco CallManager, die kritische Services sind, die auf CUCM ausgeführt werden und über entsprechende Identitätszertifikate verfügen.

Ab CUCM-Version 14 wurde eine neue Funktion hinzugefügt, um das Multi-SAN Tomcat-Zertifikat für den CallManager-Dienst wiederzuverwenden.

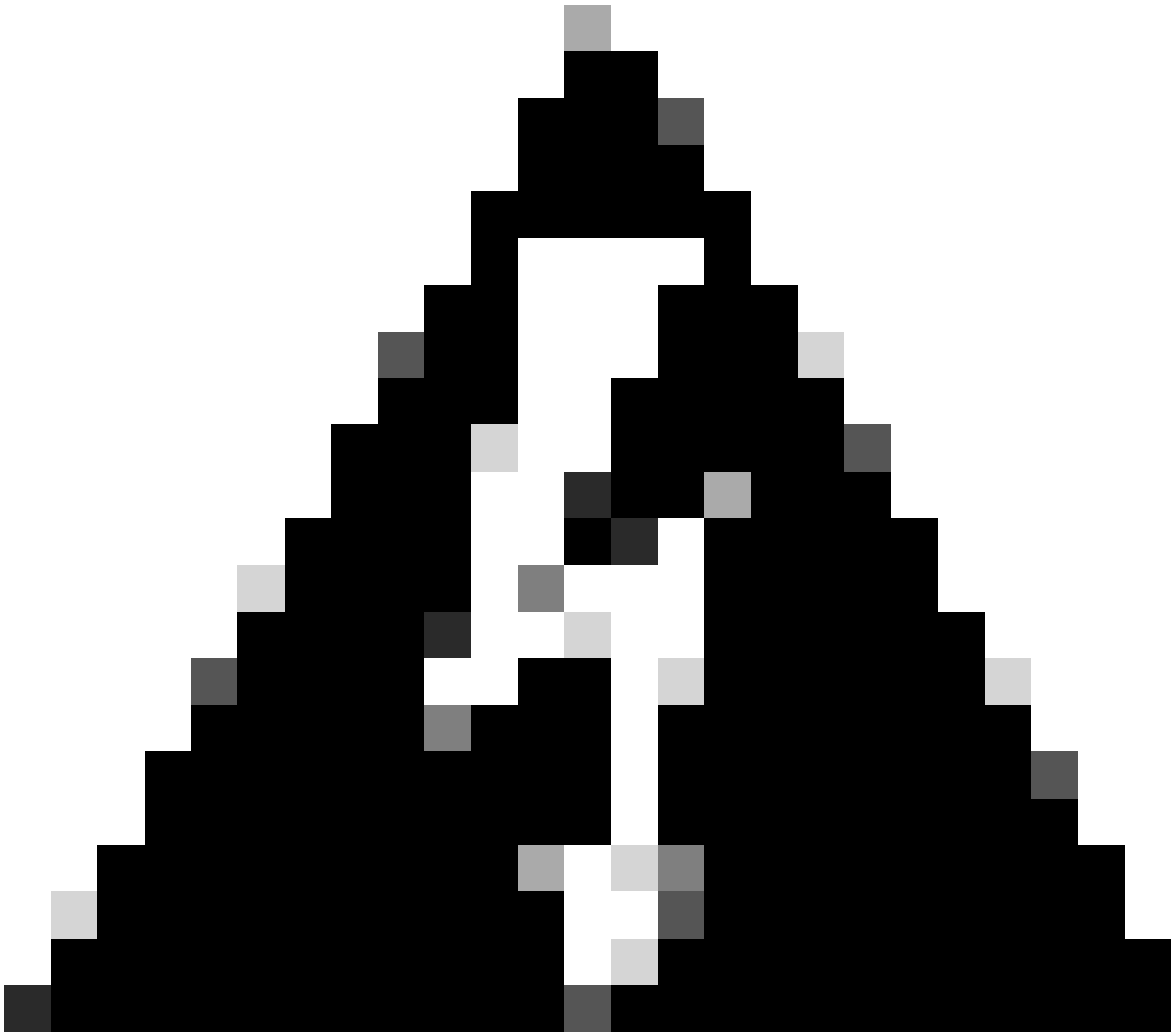
Der Vorteil dieser Funktion besteht darin, dass Sie ein Zertifikat von der Zertifizierungsstelle erhalten und es für mehrere Anwendungen verwenden können. Dies gewährleistet eine Kostenoptimierung und eine Reduzierung des Verwaltungsaufwands. Außerdem wird die Größe der ITL-Datei reduziert und somit der Overhead verringert.



Vorsicht: Bevor Sie mit der Konfiguration der Wiederverwendung fortfahren, stellen Sie sicher, dass das Tomcat-Zertifikat ein Multiserver-SAN-Zertifikat ist. Tomcat Multi-SAN-Zertifikate können selbstsigniert oder CA-signiert sein.

Konfigurieren

Tomcat-Zertifikat für CallManager wiederverwenden



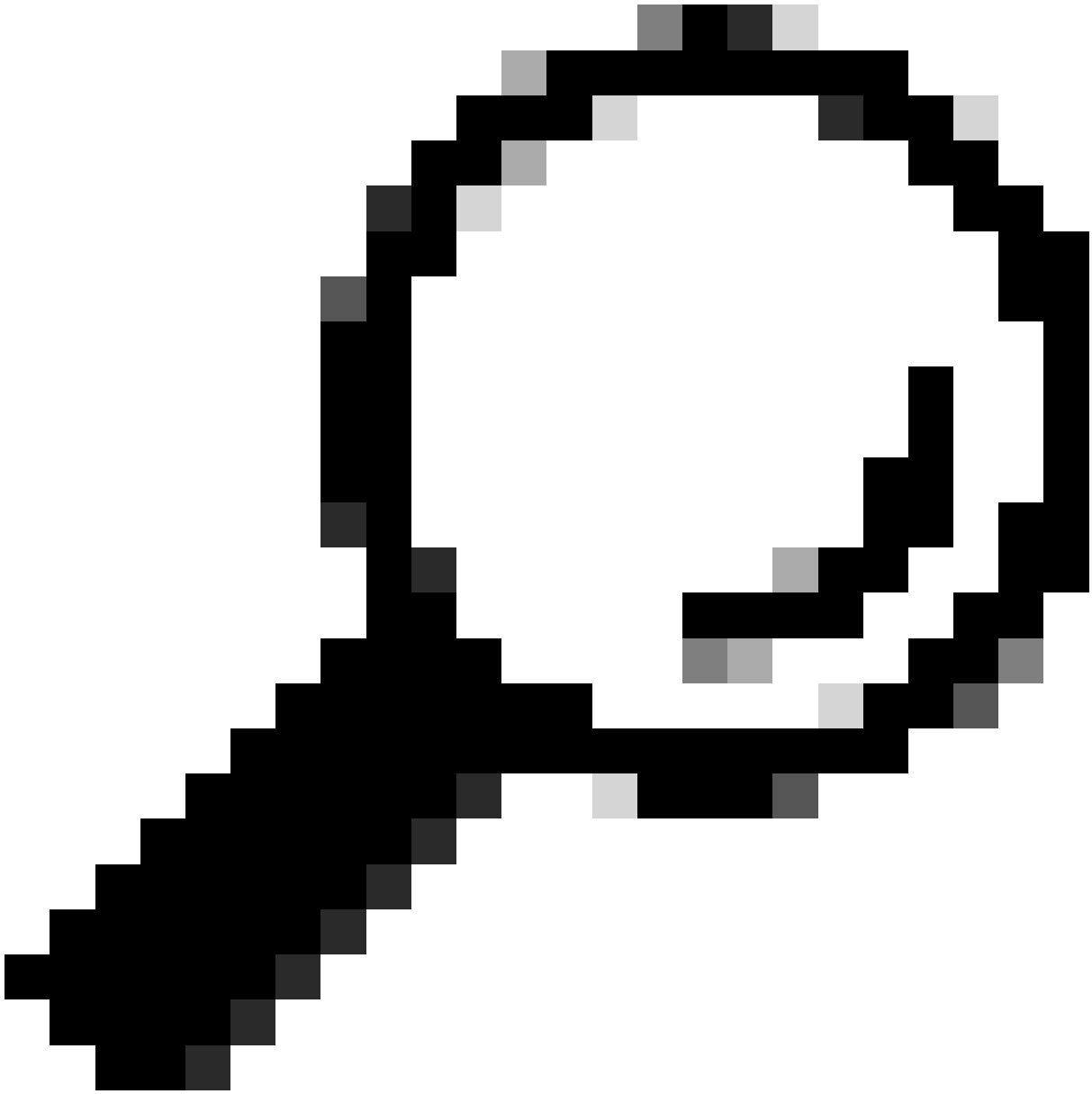
Warnung: Stellen Sie sicher, dass Sie ermittelt haben, ob sich Ihr Cluster im gemischten Modus oder im ungesicherten Modus befindet, bevor Sie fortfahren.

Schritt 1: Navigieren Sie zu Cisco Unified CM Administration > System > Enterprise Parameters:

Überprüfen Sie den Abschnitt "Sicherheitsparameter", und stellen Sie sicher, dass der Cluster-Sicherheitsmodus auf 0 oder 1 eingestellt ist. Wenn der Wert 0 ist, befindet sich der Cluster im ungesicherten Modus. Wenn der Wert 1 ist, befindet sich der Cluster im gemischten Modus, und Sie müssen die CTL-Datei vor dem Neustart der Dienste aktualisieren.

Schritt 2: Navigieren Sie zu Ihrem CUCM-Publisher und dann zu Cisco Unified OS Administration > Security > Certificate Management.

Schritt 3: Laden Sie die Multi-SAN Tomcat CA-Zertifikatskette in den CallManager Trust-Speicher hoch.



Tipp: Wenn Sie ein selbstsigniertes Multi-Server SAN-Zertifikat für Tomcat verwenden, können Sie diesen Schritt überspringen.

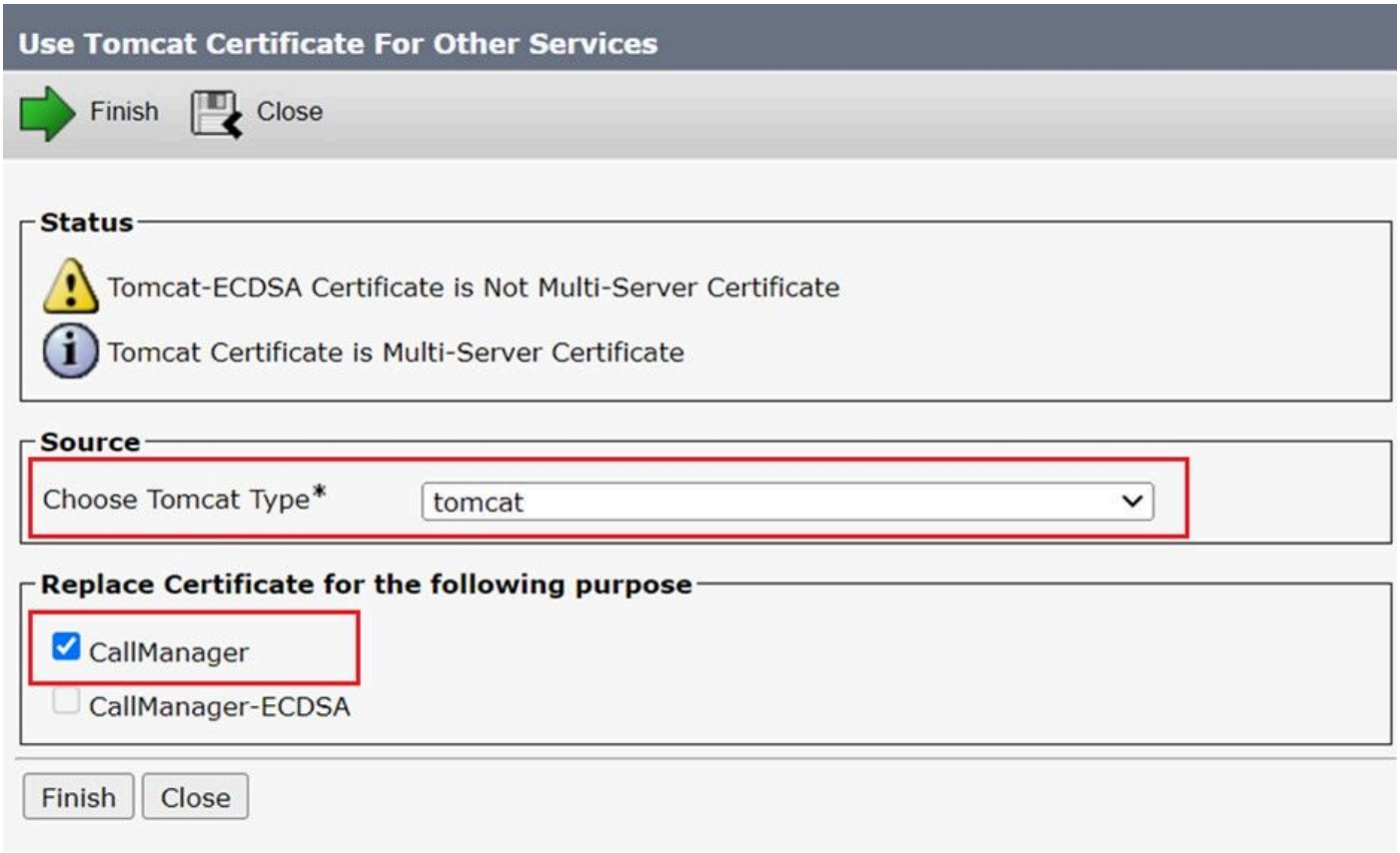
Stellen Sie vor der Wiederverwendung der Zertifikate sicher, dass Sie die Zertifikatskette der Zertifizierungsstelle (die das Tomcat-Identitätszertifikat signiert hat) manuell in den CallManager-Vertrauensspeicher hochladen.

Starten Sie diese Dienste neu, wenn Sie die Tomcat-Zertifikatskette in die CallManager-Vertrauensstellung hochladen.

- CallManager: Cisco HAProxy-Service

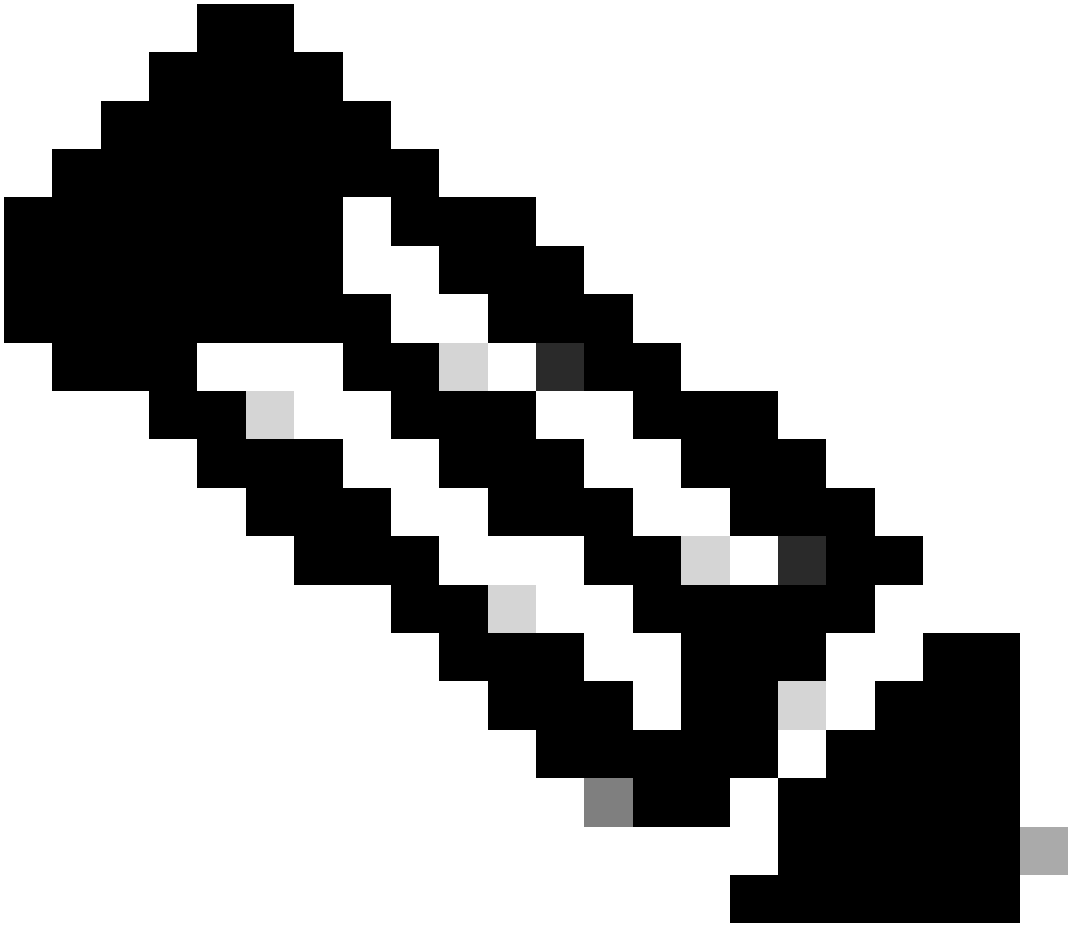
- CallManager-ECDSA: Cisco CallManager Service und Cisco HAProxy Service

Schritt 4: Klicken Sie auf Zertifikat wiederverwenden. Die Seite Tomcat-Zertifikate für andere Dienste verwenden wird angezeigt.



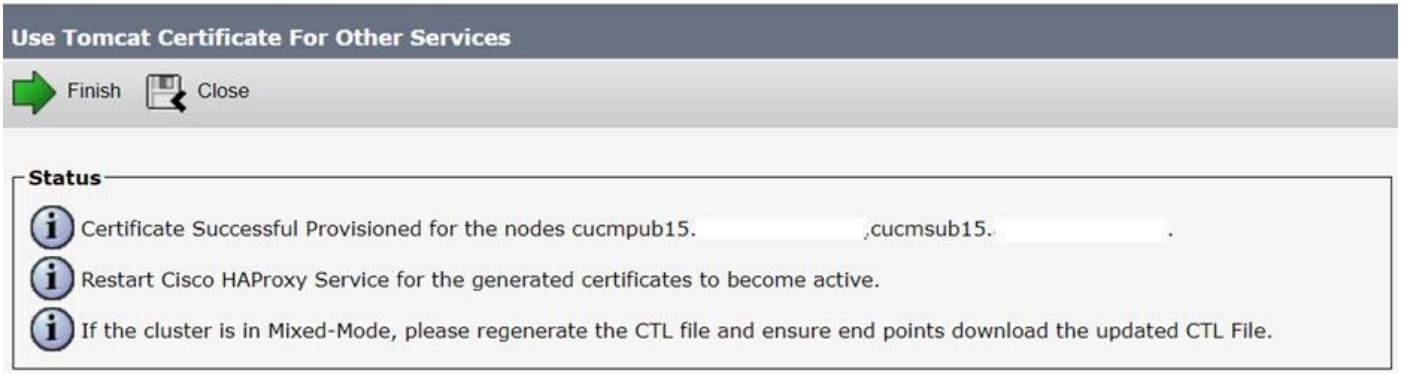
Schritt 5: Wählen Sie in der Dropdown-Liste Tomcat-Typ entweder Tomcat oder Tomcat-ECDSA aus.

Schritt 6: Aktivieren Sie im Bereich Zertifikat für folgenden Zweck ersetzen entweder das Kontrollkästchen CallManager oder CallManager-ECDSA, das auf dem zuvor ausgewählten Zertifikat basiert.

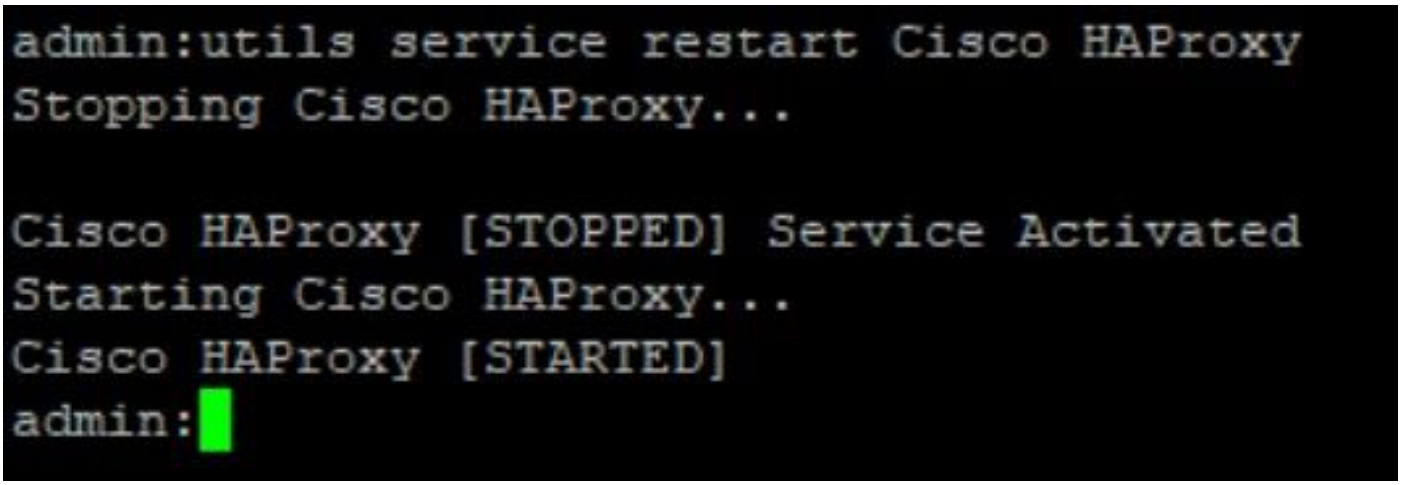


Hinweis: Wenn Sie Tomcat als Zertifikatstyp auswählen, ist CallManager als Ersatz aktiviert. Wenn Sie tomcat-ECDSA als Zertifikatstyp auswählen, wird CallManager-ECDSA als Ersatz aktiviert.

Schritt 7. Klicken Sie auf Fertig stellen, um das CallManager-Zertifikat durch das Tomcat-SAN-Zertifikat für mehrere Server zu ersetzen.

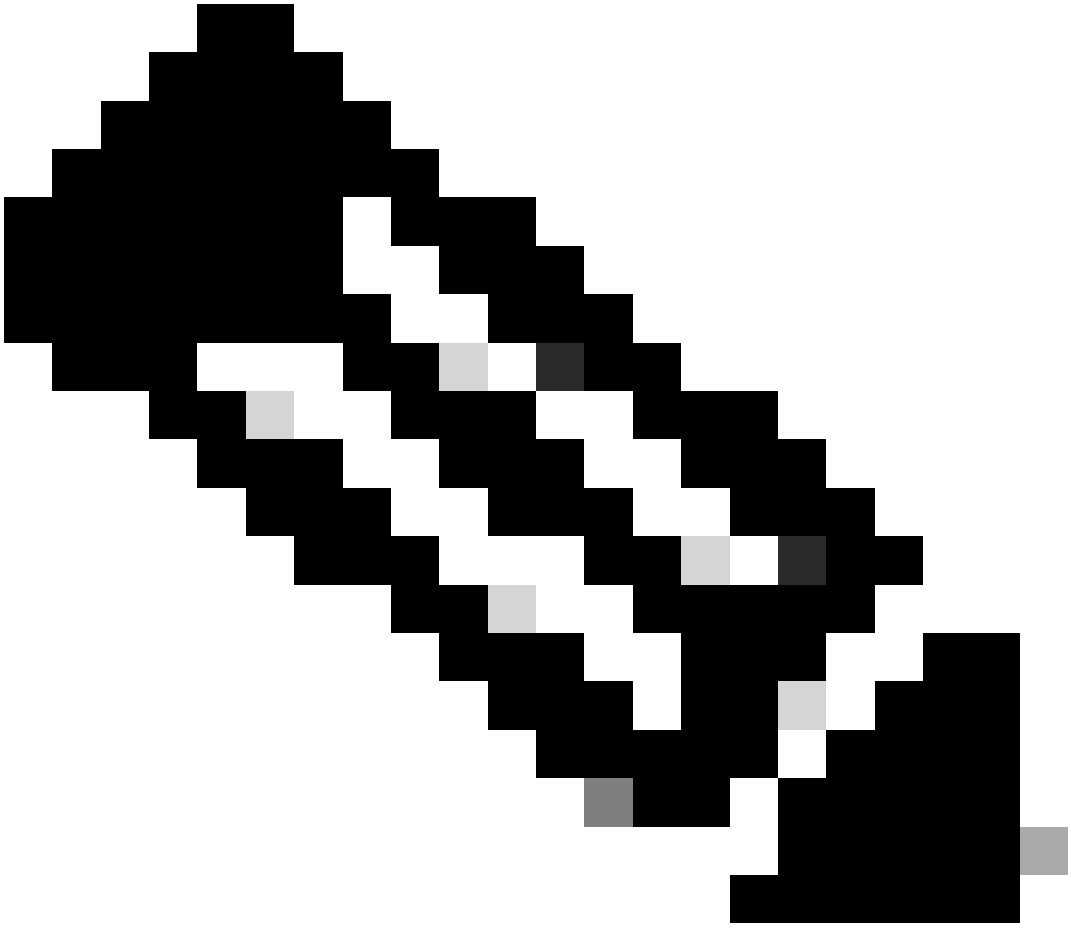


Schritt 8: Starten Sie den Cisco HAProxy-Dienst auf allen Knoten des Clusters neu, indem Sie den Befehl utils service restart Cisco HAProxy über die CLI ausführen.



Schritt 9. Wenn sich der Cluster im gemischten Modus befindet, aktualisieren Sie die CTL-Datei, indem Sie den Befehl utils ctl update CTLFile via CLI von CUCM Publisher ausführen, und setzen Sie die Telefone zurück, um die neue CTL-Datei abzurufen.

Überprüfung



Hinweis: Wenn Sie das Zertifikat wiederverwenden, wird das CallManager-Zertifikat nicht in der GUI angezeigt.

Sie können den Befehl in der CLI ausführen, um sicherzustellen, dass CallManager das Tomcat-Zertifikat wiederverwendet.

- show cert list own

```
admin:show cert list own

tomcat/tomcat.pem: Certificate Signed by AKASH-WINSERVLAB-CA
tomcat-ECDSA/tomcat-ECDSA.pem: Self-signed certificate generated by system
ipsec/ipsec.pem: Self-signed certificate generated by system
ITLRecovery/ITLRecovery.pem:
CallManager-ECDSA/CallManager-ECDSA.pem: Self-signed certificate generated by system
CallManager/CallManager.pem: Reusing tomcat certificate for CallManager
TVS/TVS.pem: Self-signed certificate generated by system


admin:
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.