Configurer la réutilisation de certificat Tomcat pour CallManager dans CUCM 14

Table des matières

Introduction

Ce document décrit comment réutiliser le certificat Multi-SAN Tomcat pour CallManager sur un serveur Cisco Unified Communications Manager (CUCM).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Certificats CUCM
- Outil de surveillance en temps réel (RTMT)
- Liste de confiance d'identité (ITL)

Composants utilisés

Les informations contenues dans ce document sont basées sur CUCM 14.0.1.13900-155.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Les deux principaux services pour CUCM sont Tomcat et CallManager. Dans les versions précédentes, des certificats différents pour chaque service étaient requis pour le cluster complet. Dans la version 14 de CUCM, une nouvelle fonctionnalité a été ajoutée pour réutiliser également le certificat Multi-SAN Tomcat pour le service CallManager. Les avantages de cette fonction sont les suivants :

- Réduit le coût d'obtention de deux certificats signés par une autorité de certification publique pour un cluster de certificats signés par une autorité de certification.
- Cette fonctionnalité réduit la taille du fichier ITL, réduisant ainsi la surcharge.

Low Impact Medium Impact. High Impact.

Type	Risk	Trust List	Impact	Phone Restart	Service Restart
Tomcat		-	Web services, SSO, EM/EMCC Login	None	Tomcat
IPSec		-	DRS, Ipsec Tunnels	None	DRF Master/Local
CAPF		CTL + ITL	LSC must be updated, secure features	All	CAPF
Callmanager		CTL + ITL	Registration, TL issues, Trunks, CTI	All	CM,CTI,TFTP
TVS		ITL	Verification of TLs, CFG files, https connection	Some	TVS
ITLRecovery		CTL + ITL	Signer or SAST backup for ITL/CTL	All	

Configurer

⚠ Mise en garde : Avant de télécharger un certificat Tomcat, vérifiez que l'authentification unique (SSO) est désactivée. Si elle est activée, l'authentification unique doit être désactivée et réactivée une fois le processus de régénération de certificat Tomcat terminé.

1. Définir le certificat Tomcat comme Multi-SAN Low Impact

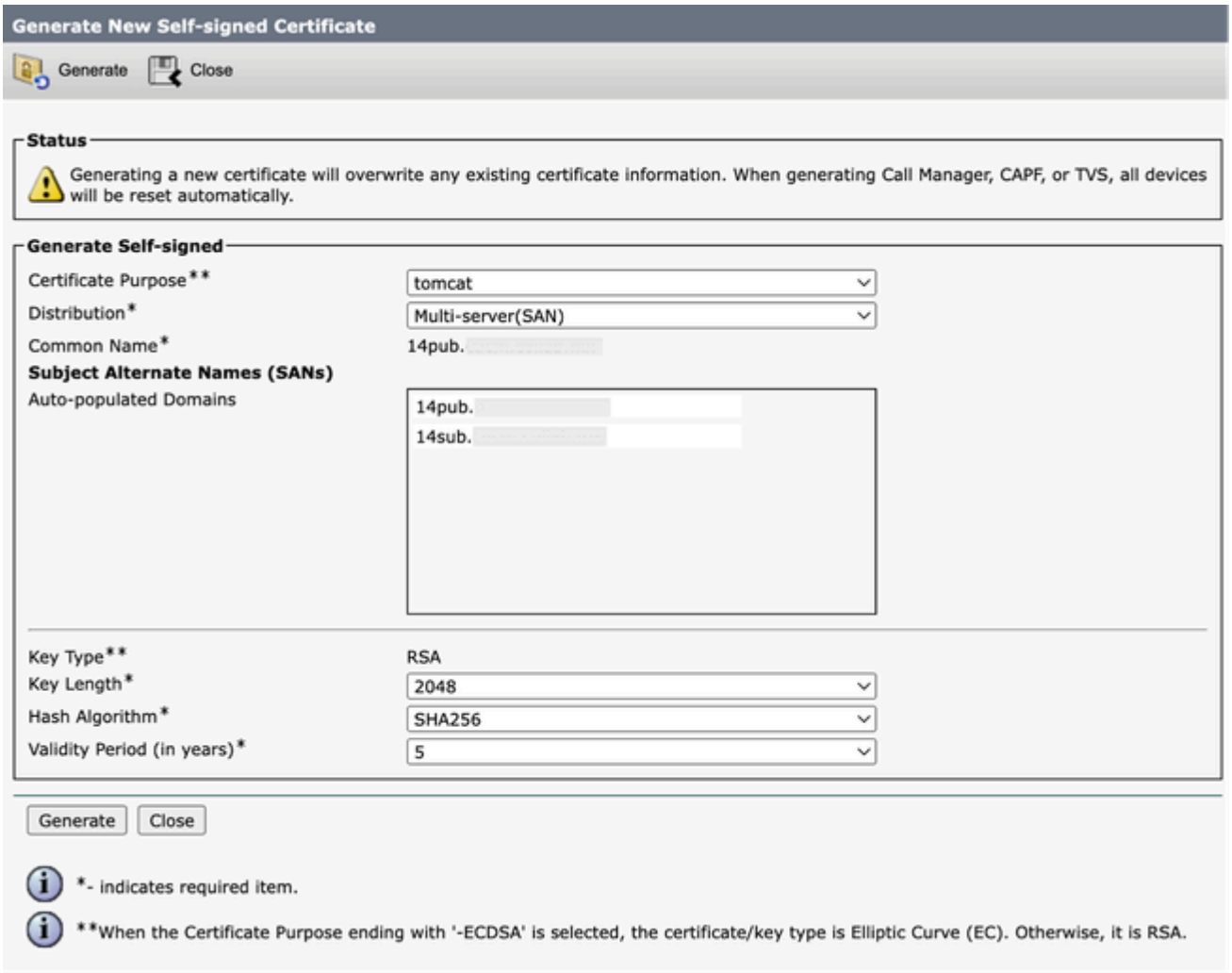
Dans CUCM 14, le certificat multi-SAN Tomcat peut être auto-signé ou signé par une autorité de certification. Si votre certificat Tomcat est déjà Multi-SAN, ignorez cette section.

Auto-signé

Étape 1. Connectez-vous à Publisher > Operating System (OS) Administration et accédez à Security > Certificate Management > Generate Self-Signed.

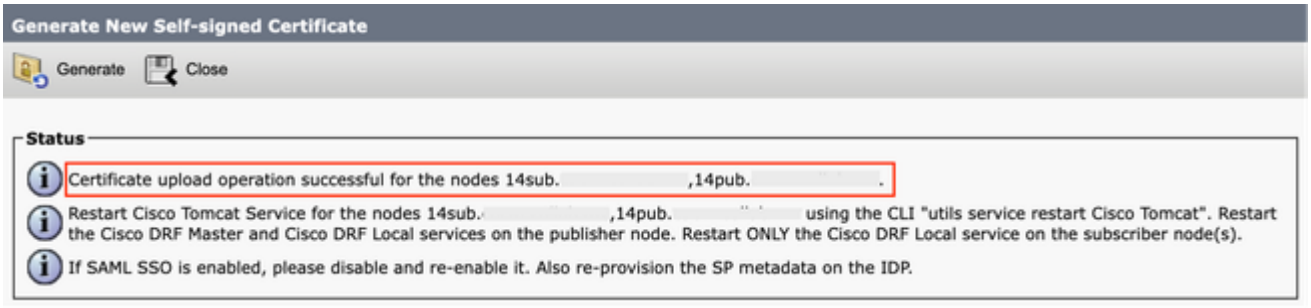
Étape 2. Choisissez Certificate Purpose: tomcat > Distribution: Multi-Server SAN. Il renseigne automatiquement les

domaines SAN et le domaine parent.



Ecran Generate Self-Signed Multi-SAN Tomcat Certificate

Étape 3. Cliquez sur Generate, puis vérifiez que tous vos noeuds sont répertoriés sous le message Certificate upload operation successful. Cliquez sur Close.



Générer un message de réussite de Tomcat multi-SAN autosigné

Étape 4. Redémarrez le service Tomcat, ouvrez une session CLI vers tous les noeuds du cluster et exécutez lautils service restart Cisco Tomcatcommande.

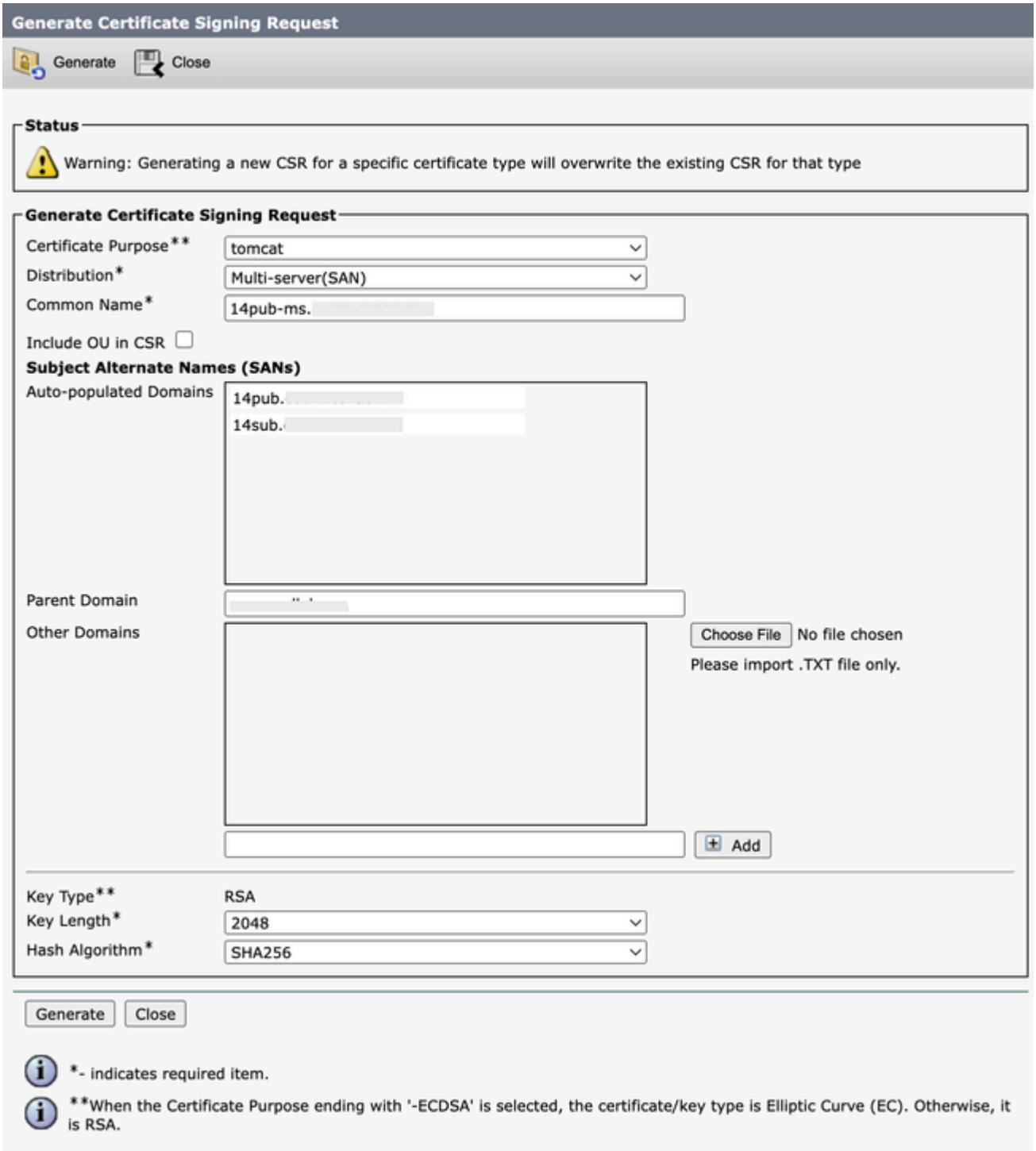
Étape 5. Accédez à la Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services et redémarrez la Cisco DRF Master Service et la Cisco DRF Local Service.

Étape 6. Accédez à chaque Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services et redémarrez Cisco DRF Local Service.

Signé par l'AC

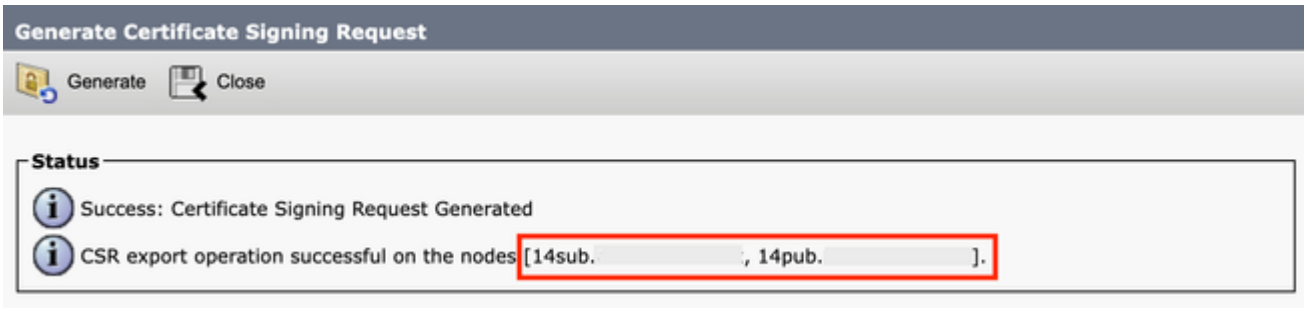
Étape 1. Connectez-vous à Publisher > Operating System (OS) Administration et accédez à Security > Certificate Management > Generate CSR.

Étape 2. Choisissez Certificate Purpose: tomcat > Distribution: Multi-Server SAN. Il renseigne automatiquement les domaines SAN et le domaine parent.



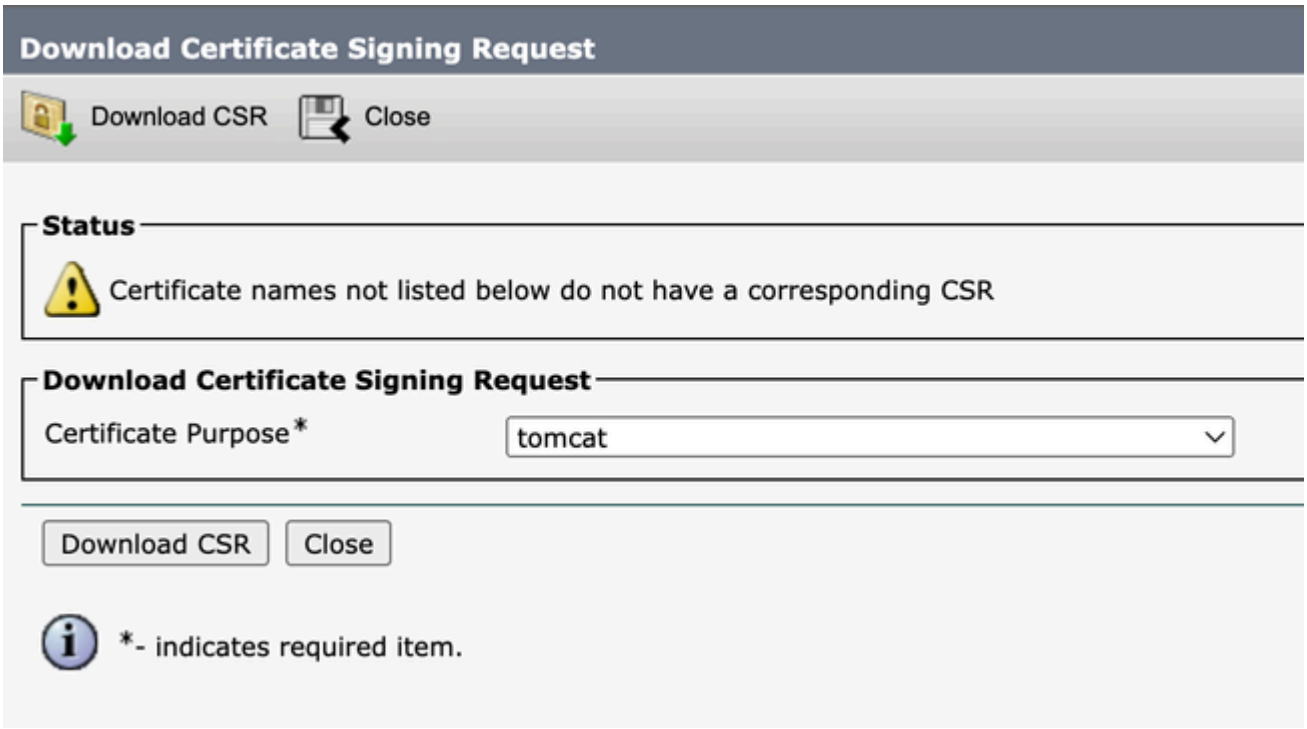
Écran Générer un CSR multi-SAN pour le certificat Tomcat

Étape 3. Cliquez sur Generate, puis validez tous vos noeuds sont répertoriés sous le message CSR export operation successful. Cliquez sur Close.



Générer un message de réussite pour Tomcat CSR multi-SAN

Étape 4. Cliquez sur Download CSR > Certificate Purpose: tomcat > Download.



Télécharger l'écran Tomcat CSR

Étape 5. Envoyez le CSR à votre autorité de certification pour signature.

Étape 6. Afin de télécharger la chaîne d'approbation CA, naviguez Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust. Définissez la description du certificat et parcourez les fichiers de la chaîne d'approbation.

Étape 7. Téléchargez le certificat signé par l'autorité de certification, accédez à Certificate Management > Upload certificate > Certificate Purpose: tomcat. Définissez la description du certificat et parcourez le fichier de certificat signé par l'autorité de certification.

utils service restart Cisco Tomcat Étape 8. Redémarrez le service Tomcat, ouvrez une session CLI sur tous les noeuds du cluster et exécutez la commande .

Étape 9. Accédez à la Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services et redémarrez

la Cisco DRF Master Service et la Cisco DRF Local Service.

Étape 10. Accédez à chaque Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services et redémarrez Cisco DRF Local Service.

2. Réutiliser le certificat Tomcat pour CallManager

Medium Impact.

⚠ Mise en garde : Pour CUCM 14, un nouveau paramètre d'entreprise Phone Interaction on Certificate Update est ajouté. Utilisez ce champ pour réinitialiser les téléphones manuellement ou automatiquement, selon le cas, lorsque l'un des certificats TVS, CAPF ou TFTP (CallManager/ITLRecovery) est mis à jour. Ce paramètre est défini par défaut sur reset the phones automatically. Après la régénération, la suppression et la mise à jour des certificats, assurez-vous que les services appropriés sont redémarrés.

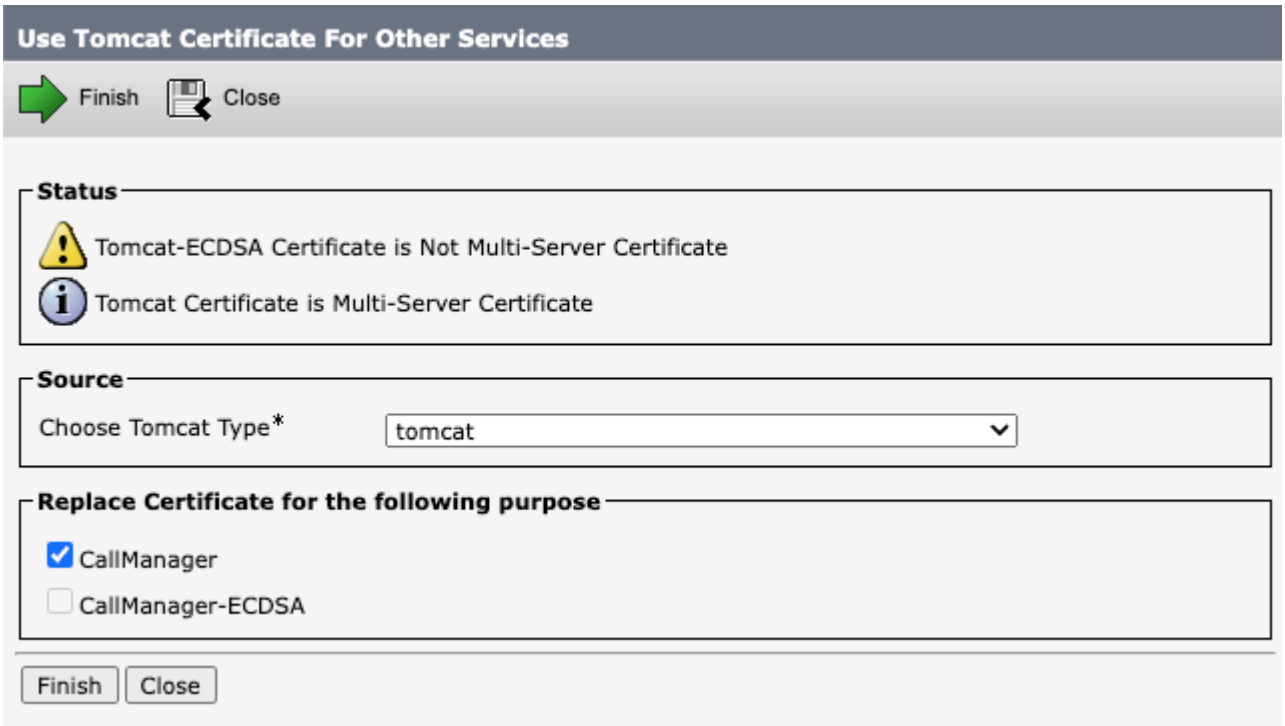
Il est nécessaire de redémarrer les services pour une régénération normale des certificats CallManager. Cochez Régénérer Les Certificats Dans Unified Communications Manager.

Étape 1. Accédez à votre éditeur CUCM, puis à Cisco Unified OS Administration > Security > Certificate Management.

Étape 2. Cliquez sur Reuse Certificate.

Étape 3. Dans la liste choose **Tomcat type** déroulante, sélectionnez tomcat.

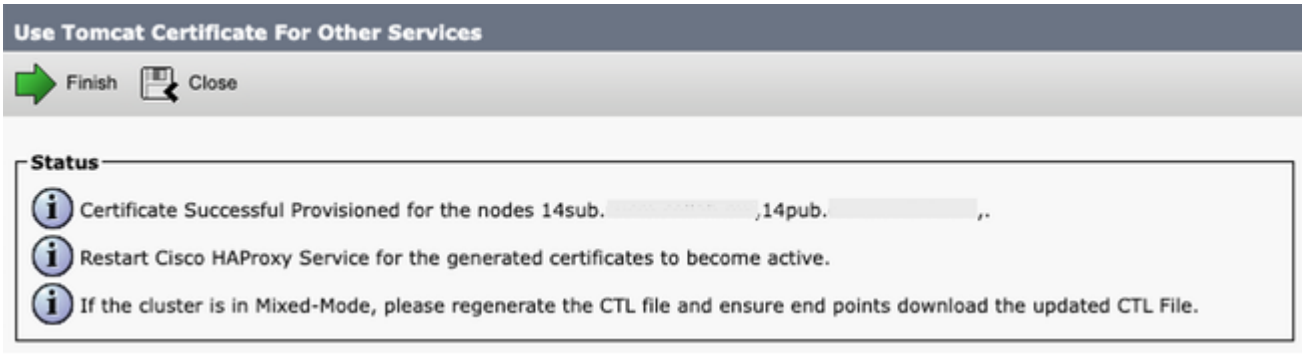
Étape 4. Dans le volet Replace Certificate for the following purpose, cochez la case à cocher CallManager.



Écran Réutiliser le certificat Tomcat pour d'autres services

Remarque : Si vous choisissez Tomcat comme type de certificat, CallManager est activé comme remplacement. Si vous choisissez tomcat-ECDSA comme type de certificat, CallManager-ECDSA est activé comme remplacement.

Étape 5. Cliquez sur Finish afin de remplacer le certificat CallManager par le certificat Tomcat Multi-SAN.



Réutiliser le message de certificat Tomcat réussi

Étape 6. Redémarrez le service Cisco HAProxy, ouvrez une session CLI vers tous les noeuds du cluster et exécutez la commande de utils service restart Cisco HAProxy .

Remarque : Afin de déterminer si le cluster est en mode mixte, accédez à Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Non-Secure ; 1 == Mixed Mode).

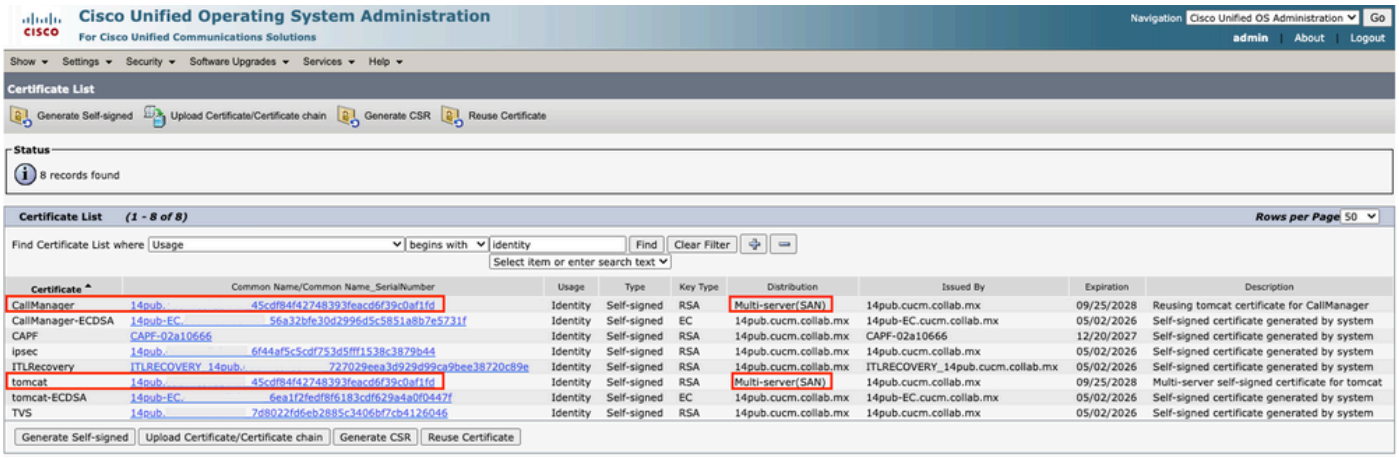
Étape 7. Si votre cluster est en mode mixte, ouvrez une session CLI sur le noeud Publisher, exécutez une **utils ctl update CTLFile** commande et réinitialisez tous les téléphones du cluster pour que les mises à jour du fichier CTL prennent effet.

Vérifier

Étape 1. Accédez à votre éditeur CUCM, puis à Cisco Unified OS Administration > Security > Certificate Management.

Étape 2. Filtrez par Find Certificate List where: Usage > begins with: identity et cliquez sur Find.

Étape 3. Les certificats CallManager et Tomcat doivent se terminer par la même Common Name_Serial Number valeur.



Vérifier la réutilisation du certificat Tomcat pour CallManager

Remarque : À partir de SU4, avec la réutilisation des certificats activée, le certificat Call Manager n'est pas affiché sur l'interface graphique utilisateur, alors que les deux certificats sont visibles dans SU2 et SU3.

Informations connexes

- Guide de sécurité pour Cisco Unified Communications Manager 14
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.