Configuration d'un autre nom de sujet multiserveur signé CA dans les systèmes CVOS

Table des matières

Introduction

Ce document décrit comment configurer un cluster de système Cisco Voice Operating System (CVOS) à l'aide d'un nom alternatif de sujet multiserveur (SAN) signé par une autorité de certification (CA) ayant un modèle d'architecture éditeur - abonné. Le système CVOS couvre les systèmes CUIC, Finesse, Livedata, IdS dans l'environnement UCCE.

Contribution de Venu Gopal Sane, Ritesh Desai Ingénieur du centre d'assistance technique Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Contact Center Enterprise (UCCE) version 12.5
- Package Cisco Contact Center Enterprise (PCCE) version v12.5
- Cisco Finesse v12.5
- Cisco Unified Intelligence Center v12.5

Composants utilisés

Les informations dans ce document sont basées sur l'administration du système d'exploitation CVOS - Gestion des certificats.

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. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

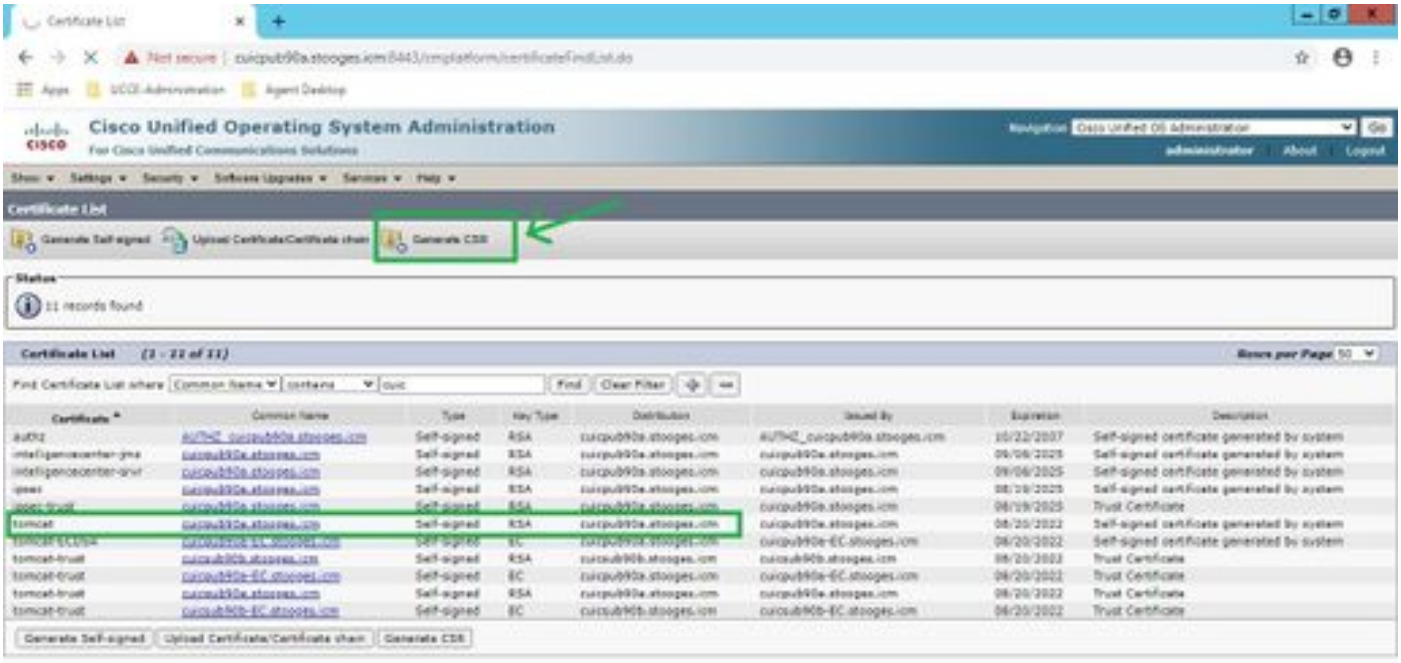
Avec les certificats SAN multiserveurs, une seule autorité de certification doit être signée par un cluster de noeuds, plutôt que d'obtenir un CSR de chaque noeud serveur du cluster, puis d'obtenir un certificat signé par l'autorité de certification pour chaque CSR et de les gérer individuellement.

Avant d'essayer cette configuration, assurez-vous que ces services sont opérationnels :

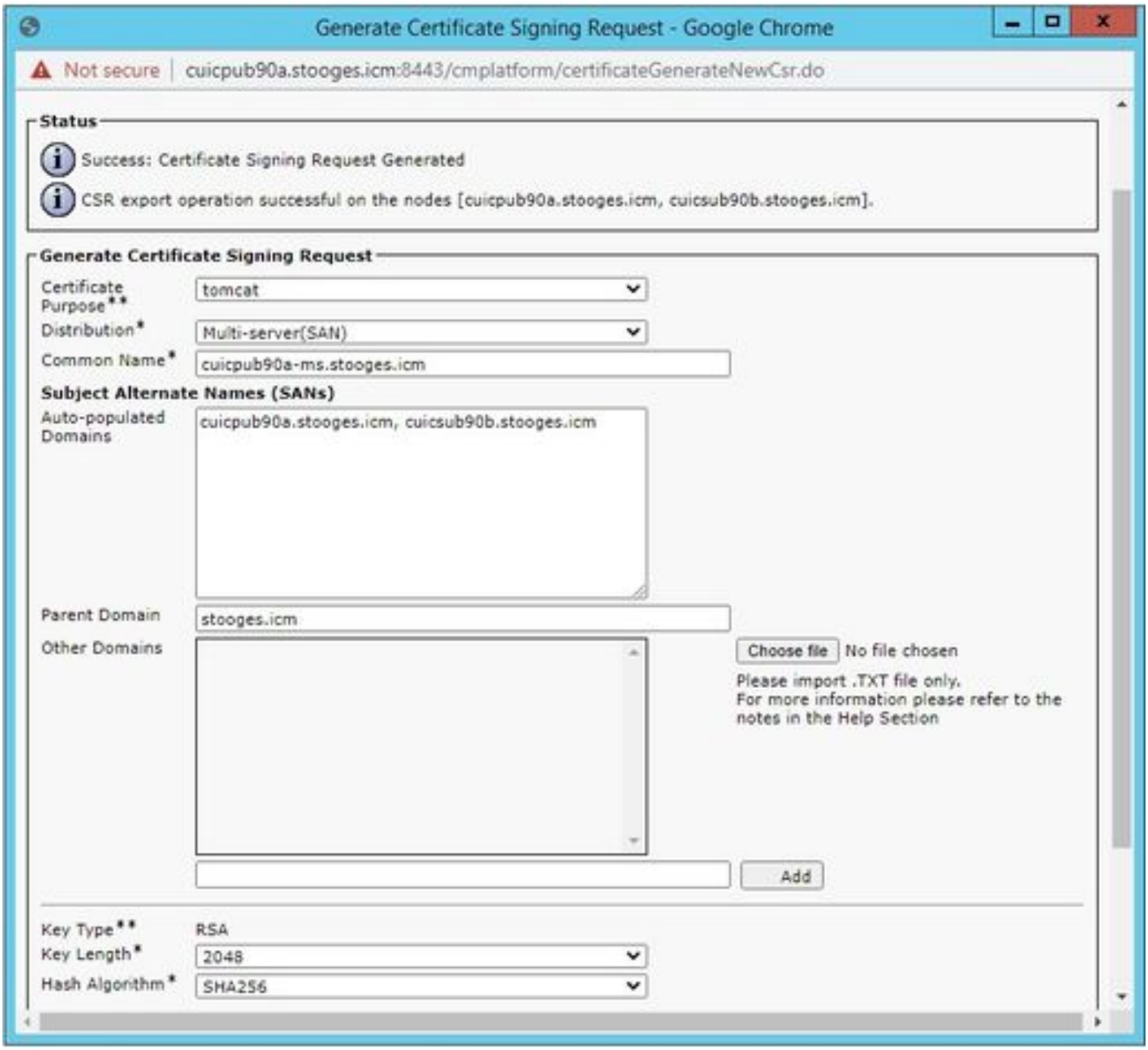
- Service Cisco Tomcat
- Notification de changement de certificat Cisco
- Cisco Certificate Expiry Monitor

Configurer

Étape 1. Connectez-vous à l'administration du système d'exploitation et accédez à Security > Certificate Management > Generate CSR comme indiqué dans l'image.

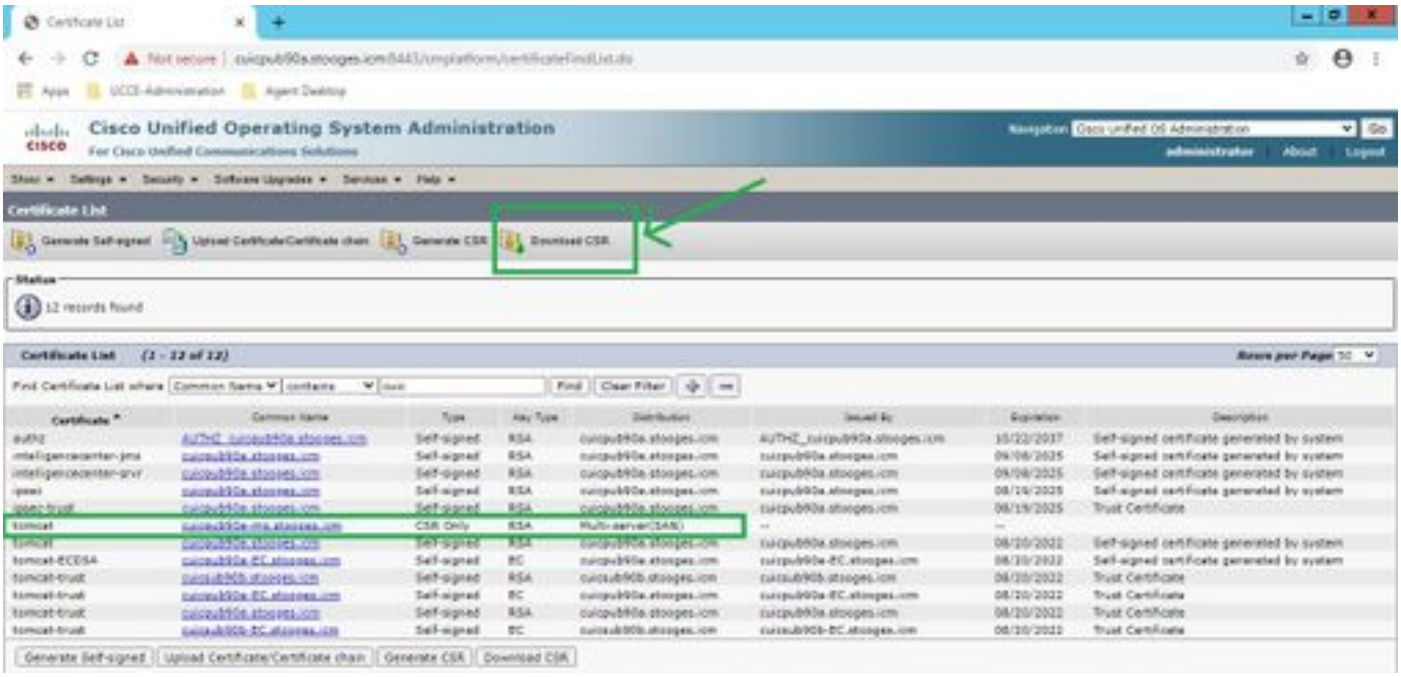


Étape 2. Sélectionnez Multi-Server SAN dans Distribution. Il remplit automatiquement les domaines SAN et le domaine parent.

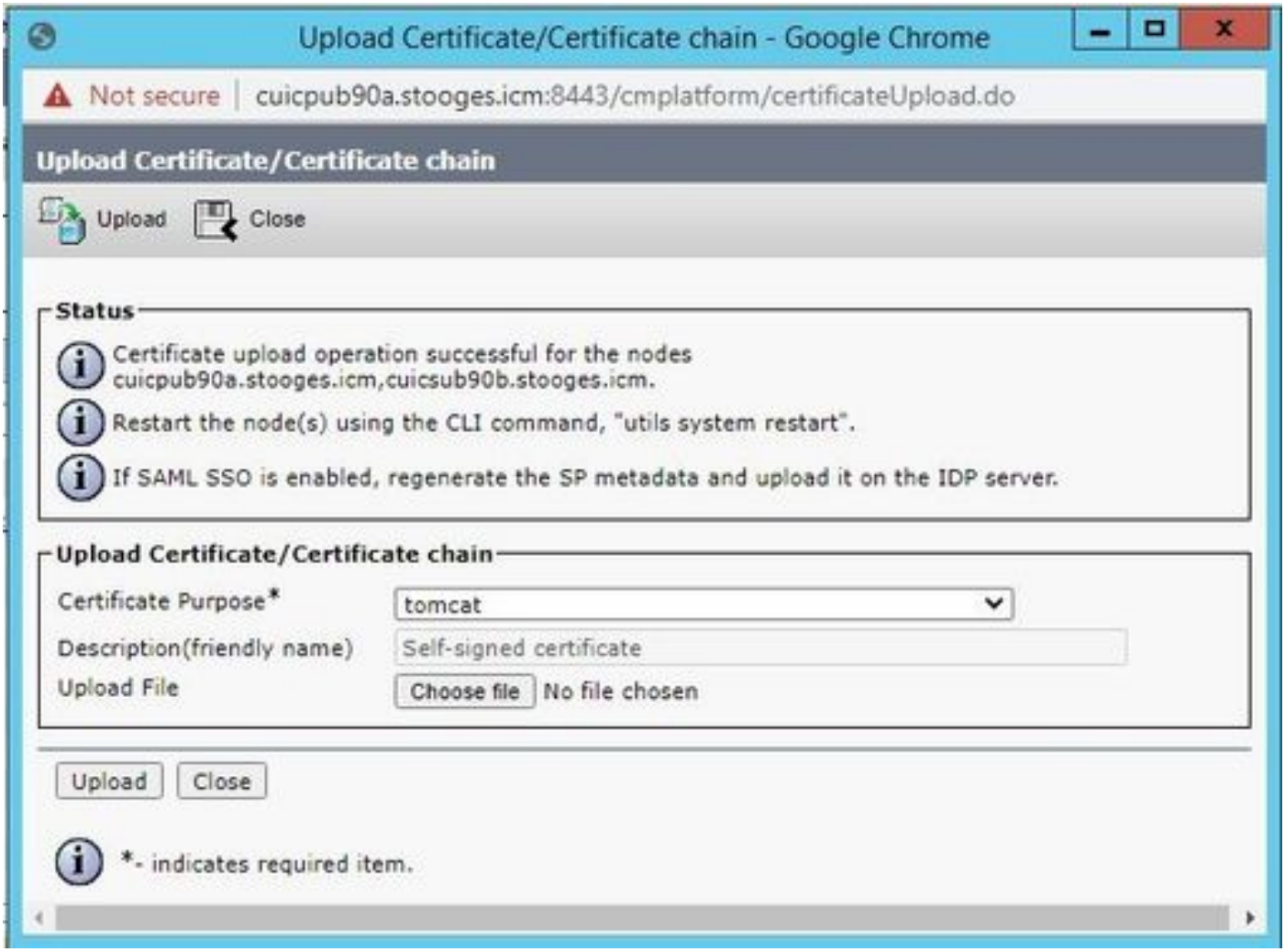


Étape 3. La génération réussie de CSR affiche le message suivant :

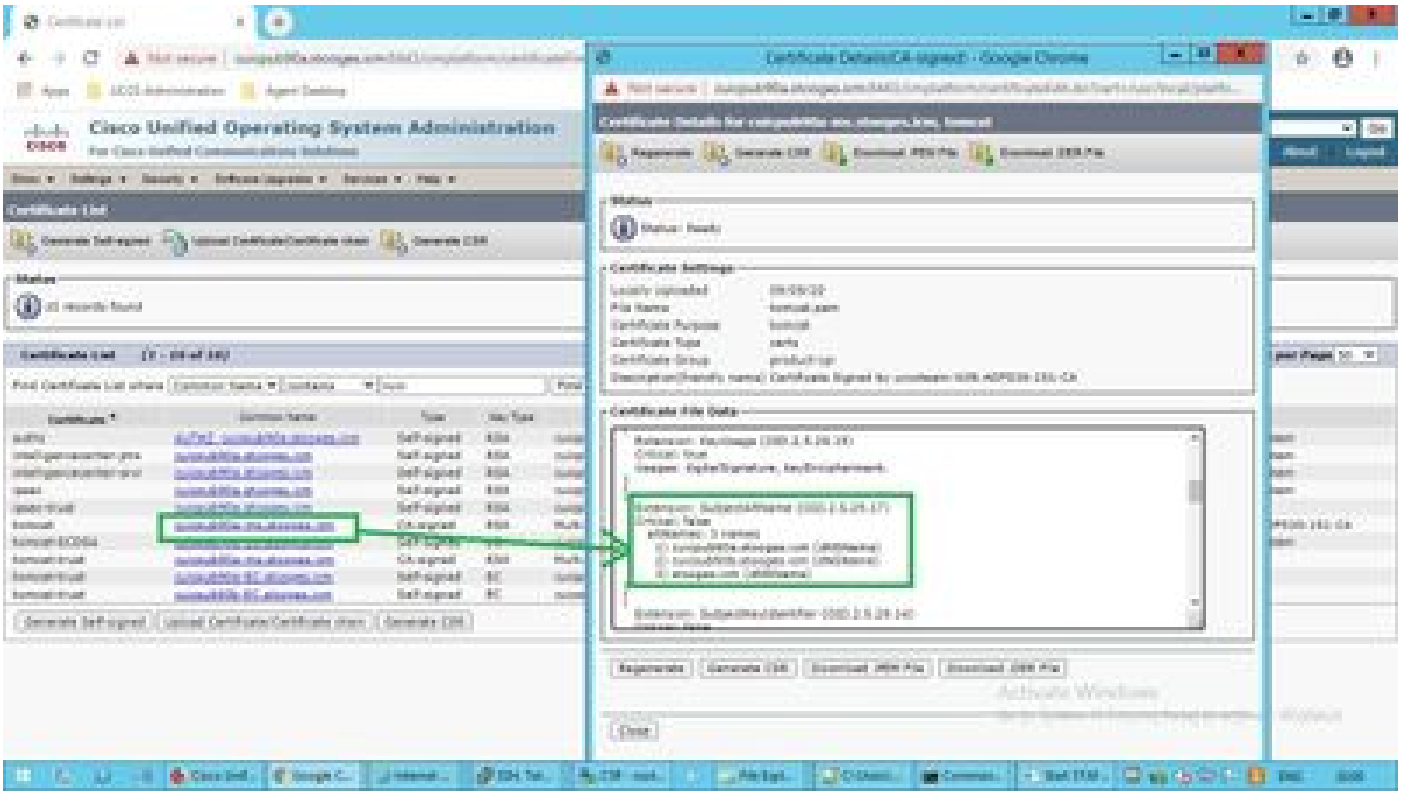
Étape 4. Une fois la CSR générée avec succès, elle est visible ici et peut être téléchargée pour être envoyée à l'autorité de certification pour signature.



Étape 5. Téléchargez le certificat signé par l'autorité de certification en tant que type tomcat dans le noeud Éditeur du cluster dans la page de gestion des certificats et suivez les instructions affichées lors du téléchargement réussi.



Étape 6. Une fois le fichier téléchargé, vérifiez la liste de certificats qui affiche le nouveau certificat signé par l'autorité de certification comme type multi-SAN.



Cliquez sur le nouveau certificat multi-SAN, vérifiez que SubjectAltNames indique le nom de domaine et les noms de domaine complets de tous les noeuds de cluster.

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Connectez-vous à la page cmplatform des noeuds de l'abonné et vérifiez que le même certificat multi-SAN est rempli avec l'utilisation de http://<any-node-fqdn>:8443/cmplatform.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Collectez ces journaux de gestion des certificats à partir de l'accès CLI et ouvrez le dossier avec Cisco TAC : file get activelog platform/log/cert*

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.