

Implémenter la réutilisation du certificat Tomcat multi-SAN pour CallManager

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Réutiliser le certificat Tomcat pour CallManager](#)

[Vérifier](#)

Introduction

Ce document décrit un processus étape par étape sur la façon de réutiliser le certificat Multi-SAN Tomcat pour CallManager sur CUCM.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestionnaire de communications unifiées de Cisco (version CUCM)
- Certificats CUCM
- Liste de confiance d'identité (ITL)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CUCM version 15 SU1

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.

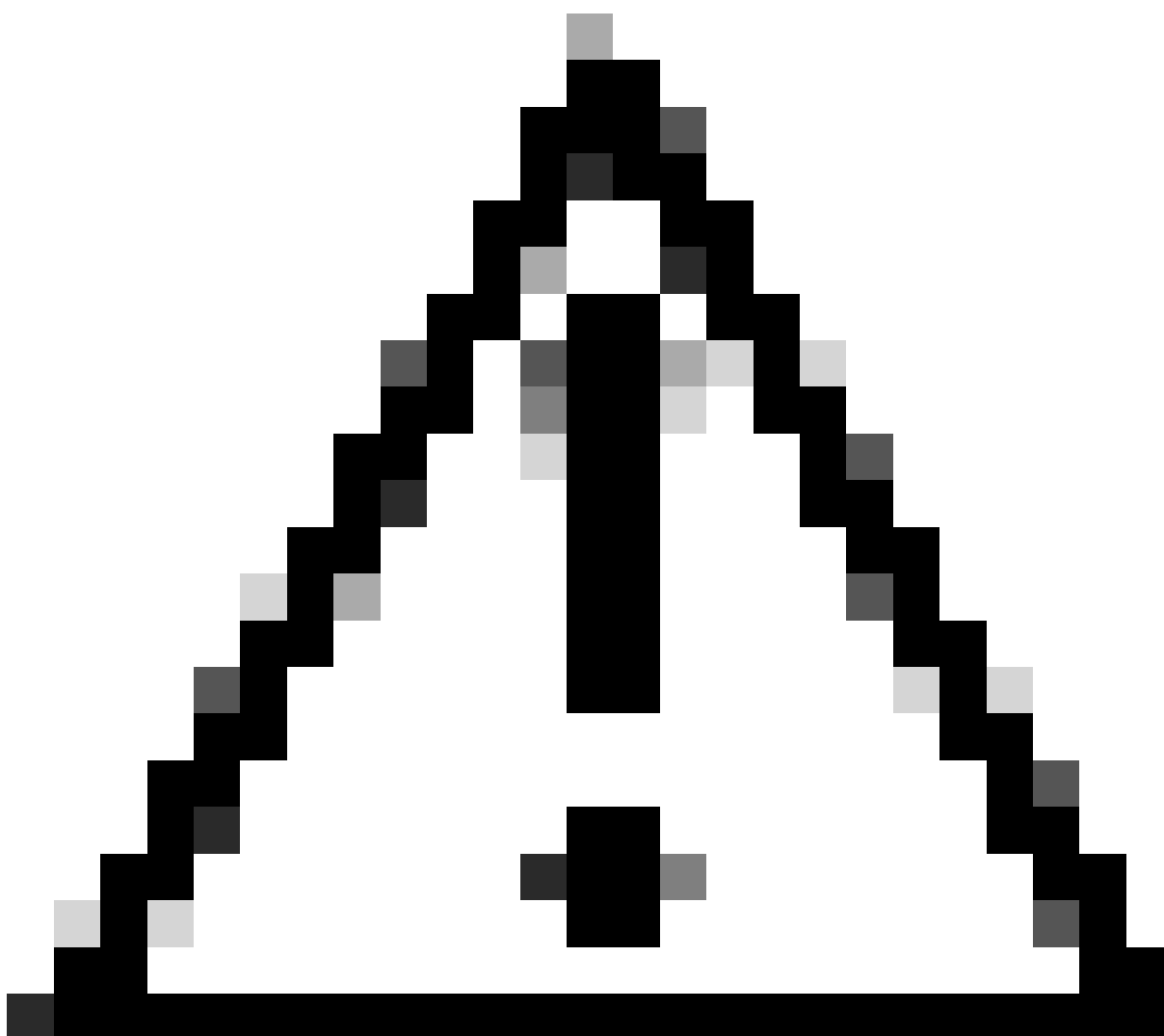
Informations générales

Les versions antérieures de CUCM utilisaient des certificats différents pour chaque service pour le

cluster complet, ce qui augmentait le nombre de certificats et le coût. Cela inclut Cisco Tomcat et Cisco CallManager, qui sont des services critiques exécutés sur CUCM et qui possèdent également des certificats d'identité respectifs.

À partir de la version 14 de CUCM, une nouvelle fonctionnalité a été ajoutée pour réutiliser le certificat Multi-SAN Tomcat pour le service CallManager.

L'avantage de cette fonctionnalité est que vous pouvez obtenir un certificat auprès de l'autorité de certification et l'utiliser dans plusieurs applications. Cela garantit une optimisation des coûts et une réduction de la gestion, et réduit la taille du fichier ITL, réduisant ainsi les frais généraux.



Attention : avant de poursuivre la configuration de réutilisation, assurez-vous que le certificat Tomcat est un certificat SAN multiserveur. Le certificat multi-SAN Tomcat peut être auto-signé ou signé par une autorité de certification.

Configurer

Réutiliser le certificat Tomcat pour CallManager



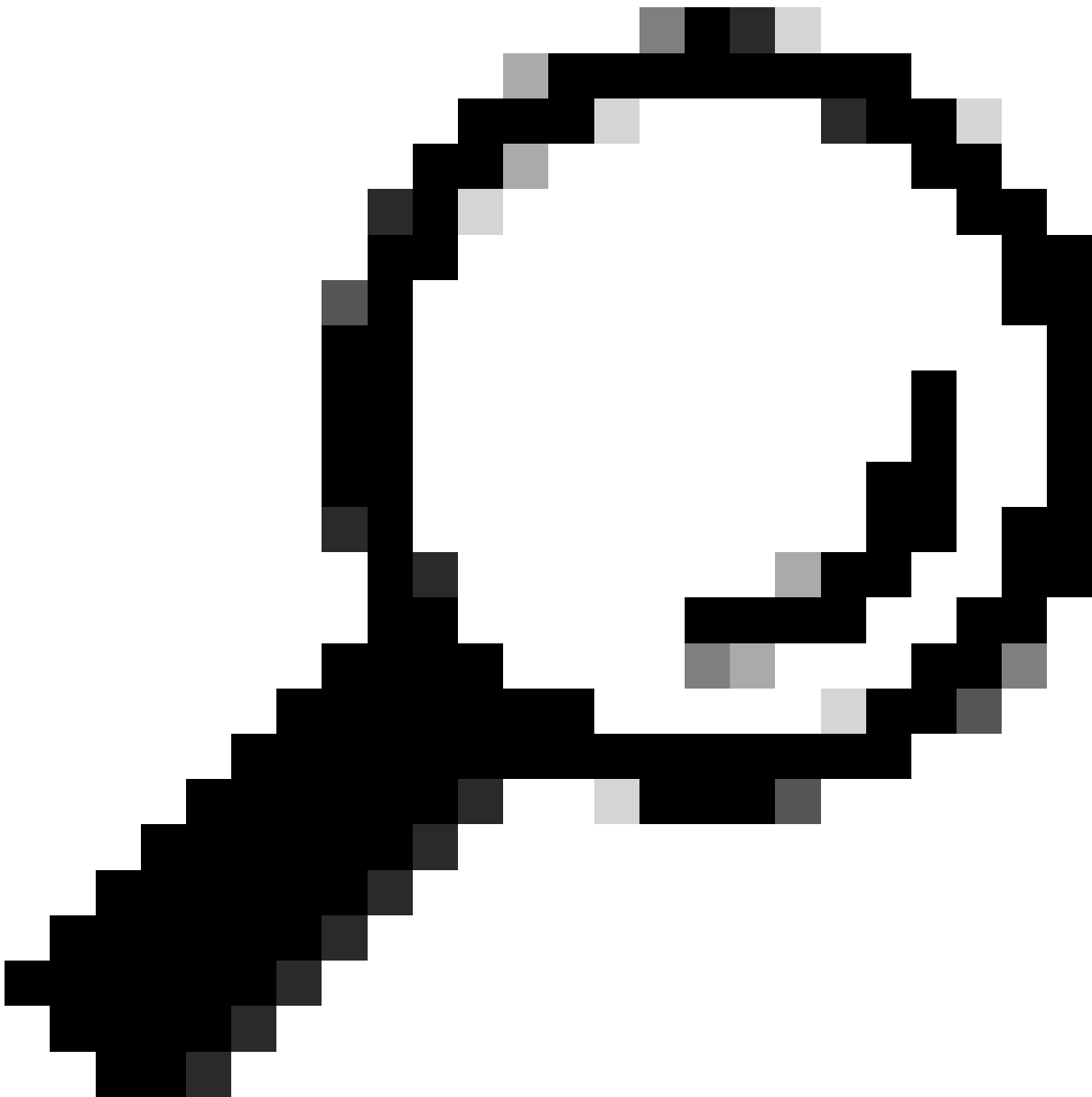
Avertissement : vérifiez que vous avez identifié si votre cluster est en mode mixte ou non sécurisé avant de continuer.

Étape 1. Accédez à Cisco Unified CM Administration > System > Enterprise Parameters :

Consultez la section Paramètres de sécurité et vérifiez si le mode de sécurité du cluster est défini sur 0 ou 1. Si la valeur est 0, le cluster est en mode non sécurisé. Si la valeur est 1, le cluster est en mode mixte et vous devez mettre à jour le fichier CTL avant le redémarrage des services.

Étape 2. Accédez à votre éditeur CUCM, puis à Cisco Unified OS Administration > Security > Certificate Management.

Étape 3. Téléchargez la chaîne de certificats CA Tomcat multi-SAN vers le magasin de confiance CallManager.



Conseil : si vous utilisez un certificat SAN multiserveur auto-signé pour Tomcat, vous pouvez ignorer cette étape.

Avant de réutiliser les certificats, assurez-vous de télécharger manuellement la chaîne de certificats de l'autorité de certification (qui a signé le certificat d'identité tomcat) vers le magasin de confiance CallManager.



Redémarrez ces services lorsque vous téléchargez la chaîne de certificats tomcat vers l'approbation CallManager.

- CallManager : service Cisco HAProxy
- CallManager-ECDSA : service Cisco CallManager et service Cisco HAProxy



Étape 4. Cliquez sur Réutiliser le certificat. La page Utiliser les certificats Tomcat pour d'autres

services s'affiche.

Use Tomcat Certificate For Other Services

 Finish  Close

Status

 Tomcat-ECDSA Certificate is Not Multi-Server Certificate
 Tomcat Certificate is Multi-Server Certificate

Source

Choose Tomcat Type*

Replace Certificate for the following purpose

CallManager
 CallManager-ECDSA

Étape 5. Dans la liste déroulante Type Tomcat, sélectionnez Tomcat ou Tomcat-ECDSA.



Étape 6. Dans le volet Remplacer le certificat pour l'objectif suivant, cochez la case CallManager ou CallManager-ECDSA en fonction du certificat sélectionné à l'étape précédente.






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 7. Cliquez sur Finish pour remplacer le certificat CallManager par le certificat SAN multiserveur Tomcat.

Use Tomcat Certificate For Other Services

 Finish  Close

Status

-  Certificate Successful Provisioned for the nodes cucmpub15. ,cucmsub15. .
-  Restart Cisco HAProxy Service for the generated certificates to become active.
-  If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.

Étape 8. Redémarrez le service Cisco HAProxy sur tous les noeuds du cluster en exécutant la commande `utils service restart Cisco HAProxy` via l'interface de ligne de commande.

```
admin:utils service restart Cisco HAProxy
Stopping Cisco HAProxy...

Cisco HAProxy [STOPPED] Service Activated
Starting Cisco HAProxy...
Cisco HAProxy [STARTED]
admin:█
```

Étape 9. Si le cluster est en mode mixte, mettez à jour le fichier CTL en exécutant la commande `utils ctl update CTLFile` via CLI de CUCM Publisher et continuez à réinitialiser les téléphones pour obtenir le nouveau fichier CTL.

Vérifier

Remarque : le certificat CallManager n'est pas affiché sur l'interface utilisateur graphique lorsque vous réutilisez le certificat.

Vous pouvez exécuter la commande à partir de l'interface de ligne de commande pour confirmer que CallManager réutilise le certificat Tomcat.

- 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:█
```


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.