

Régénérer les certificats auto-signés de service IM/P CUCM

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Utilisation du magasin de certificats](#)

[Certificat Cisco Unified Presence \(CUP\)](#)

[Cisco Unified Presence - Certificat CUP-XMPP \(Extensible Messaging and Presence Protocol\)](#)

[Cisco Unified Presence - Extensible Messaging and Presence Protocol - Certificat de serveur à serveur \(CUP-XMPP-S2S\)](#)

[Certificat de sécurité IP \(IPSec\)](#)

[Certificat Tomcat](#)

[Processus de régénération de certificat](#)

[Certificat CUP](#)

[Certificat CUP-XMPP](#)

[Certificat CUP-XMPP-S2S](#)

[Certificat IPSec](#)

[Certificat Tomcat](#)

[Supprimer les certificats de confiance expirés](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit une procédure recommandée étape par étape sur la façon de régénérer les certificats dans CUCM IM/P 8.x et versions ultérieures.

Conditions préalables

Exigences

Cisco recommande que vous ayez connaissance des certificats de service IM & Presence (IM/P).

Composants utilisés

Les informations contenues dans ce document sont basées sur la version 8.x et les versions ultérieures de IM/P.

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

Utilisation du magasin de certificats

Certificat Cisco Unified Presence (CUP)

Utilisé pour les connexions SIP sécurisées pour la fédération SIP, le contrôle d'appel à distance Microsoft pour Lync/OCS/LCS, la connexion sécurisée entre Cisco Unified Certificate Manager (CUCM) et IM/P, etc.

Cisco Unified Presence - Certificat CUP-XMPP (Extensible Messaging and Presence Protocol)

Utilisé pour valider les connexions sécurisées pour les clients XMPP lors de la création d'une session XMPP.

Cisco Unified Presence - Extensible Messaging and Presence Protocol - Certificat de serveur à serveur (CUP-XMPP-S2S)

Utilisé pour valider les connexions sécurisées pour les fédérations interdomaines XMPP avec un système XMPP fédéré en externe.

Certificat de sécurité IP (IPSec)

Utilisé pour :

- Valider une connexion sécurisée pour le système de reprise après sinistre (DRS)/le cadre de reprise après sinistre (DRF)
- Valider une connexion sécurisée pour les tunnels IPsec vers Cisco Unified Communications Manager (CUCM) et les noeuds IM/P du cluster

Certificat Tomcat

Utilisé pour :

- Validez divers accès Web, tels que l'accès aux pages de service à partir d'autres noeuds du cluster et Jabber Access.
- Validez la connexion sécurisée pour l'authentification unique (SSO) SAML.
- Validez la connexion sécurisée pour l'homologue intercluster.



Attention : si vous utilisez la fonctionnalité SSO sur vos serveurs Unified Communication et que les certificats Cisco Tomcat sont régénérés, l'authentification unique doit être reconfigurée avec les nouveaux certificats. Le lien pour configurer SSO sur CUCM et ADFS 2.0 est : <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html>.



Remarque : le lien vers le processus de renouvellement/régénération de certificat CUCM est le suivant :

<https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/200199-CUCM-Certificate-Regeneration-Renewal-Pr.html>.

Processus de régénération de certificat

Certificat CUP

Étape 1. Ouvrez une interface graphique utilisateur (GUI) pour chaque serveur de votre cluster. Commencez par l'éditeur IM/P, puis ouvrez successivement une interface utilisateur graphique pour chaque serveur d'abonnés IM/P et accédez à Cisco Unified OS Administration > Security > Certificate Management.

Étape 2. Commencez par l'interface utilisateur graphique de l'éditeur et choisissez Find d'afficher tous les certificats. Sélectionnez le certificatcup.pem. Une fois ouvert, choisissez Regenerate et attendez que la fenêtre contextuelle soit fermée pour voir si le message a réussi.

Étape 3. Continuez avec les abonnés suivants, reportez-vous à la même procédure qu'à l'étape 2. et complétez tous les abonnés de votre cluster.

Étape 4. Une fois le certificat CUP régénéré sur tous les noeuds, les services doivent être redémarrés.



Remarque : si la case Activer la haute disponibilité est cochée dans la configuration Presence Redundancy Group, vérifiezUncheck-la avant de redémarrer les services. La configuration du groupe de redondance de présence est accessible à l'adresse CUCM Pub Administration > System > Presence Redundancy Group. Un redémarrage des services entraîne une interruption temporaire de la messagerie instantanée et doit être effectué en dehors des heures de production.

Redémarrez les services dans cet ordre :

· Connectez-vous à Cisco Unified Serviceability de l'éditeur :

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Service proxy SIP Restart Cisco.

c. Une fois le redémarrage du service terminé, poursuivez avec les abonnés et le service Cisco SIP ProxyRestart.

d. Commencez par l'éditeur, puis continuez avec les abonnés. Restart Service Cisco SIP Proxy (également, à partir de Cisco Unified Serviceability > Tools > Control Center - Feature Services).

· Connectez-vous à Cisco Unified Serviceability de l'éditeur :

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. ServiceRestart Cisco Presence Engine.

c. Une fois le redémarrage du service terminé, passez à Restart du service Cisco Presence Engine sur les abonnés.



Remarque : s'il est configuré pour la fédération SIP, Restart le service Cisco XCP SIP Federation Connection Manager (situé à l'adresse Cisco Unified Serviceability > Tools > Control Center - Feature Services). Commencez par l'éditeur, puis continuez avec les abonnés.

Certificat CUP-XMPP



Remarque : étant donné que Jabber utilise les certificats de serveur CUCM et IM/P Tomcat et CUP-XMPP pour valider les connexions pour Tomcat et les services CUP-XMPP, ces certificats CUCM et IM/P sont dans la plupart des cas signés CA. Supposons que le périphérique Jabber ne dispose pas de la racine et d'un certificat intermédiaire qui fait partie du certificat CUP-XMPP installé dans son



magasin de certificats de confiance. Dans ce cas, le client Jabber affiche une fenêtre contextuelle d'avertissement de sécurité pour le certificat non approuvé. S'il n'est pas déjà installé dans le certificat du magasin d'approbation de périphérique Jabber, le certificat racine et tout certificat intermédiaire doivent être transmis au périphérique Jabber via la stratégie de groupe, MDM, e-mail, etc., qui dépend du client Jabber.



Remarque : si le certificat CUP-XMPP est auto-signé, le client Jabber affiche une fenêtre contextuelle d'avertissement de sécurité pour le certificat non approuvé si le certificat CUP-XMPP n'est pas installé dans le magasin de confiance du certificat de périphérique Jabber. S'il n'est pas déjà installé, le certificat auto-signé CUP-XMPP doit être envoyé au périphérique Jabber via la stratégie de groupe, MDM, e-mail, etc., qui dépend du client Jabber.

Étape 1. Ouvrez une interface utilisateur graphique pour chaque serveur de votre cluster. Commencez par l'éditeur IM/P, puis ouvrez successivement une interface utilisateur graphique pour chaque serveur d'abonnés IM/P et accédez à **Cisco Unified OS Administration > Security > Certificate Management**.

Étape 2. Commencez par l'interface utilisateur graphique de l'éditeur et choisissez Find d'afficher tous les certificats. À partir de la colonne type du cup-xmpp.pem certificat, déterminez s'il est auto-signé ou signé par une autorité de certification. Si le cup-xmpp.pem certificat est un multi-SAN de distribution signé par un tiers (type signé par une autorité de certification), passez en revue ce lien lorsque vous générez un CSR CUP-XMPP multi-SAN et soumettez à l'autorité de certification le certificat CUP-XMPP signé par une autorité de certification ; [Exemple de configuration d'une configuration de cluster de communications unifiées avec un nom alternatif d'objet multi-serveur signé par une autorité de certification](#).

Si le cup-xmpp.pem certificat est un noeud unique de distribution signé par un tiers (type signé par une autorité de certification) (le nom de distribution correspond au nom commun du certificat), consultez ce lien lorsque vous générez un CUP-XMPP CSR à noeud unique et que vous l'envoyez à l'autorité de certification pour le certificat CUP-XMPP signé par une autorité de certification ; [Guide pratique complet de Jabber pour la validation du certificat](#). Si le cup-xmpp.pem certificat est auto-signé, passez à l'étape 3.

Étape 3. Choisissez Find afin d'afficher tous les certificats, puis choisissez le certificat de votre cup-xmpp.pem choix. Une fois ouvert, choisissez Regenerate et attendez que la fenêtre contextuelle soit fermée pour voir si le message a réussi.

Étape 4. Continuez avec les abonnés suivants ; reportez-vous à la même procédure à l'étape 2 et effectuez-la pour tous les abonnés de votre cluster.

Étape 5. Une fois que le certificat CUP-XMPP a été régénéré sur tous les noeuds, le service du routeur Cisco XCP doit être redémarré sur les noeuds IM/P.



Remarque : si la case Activer la haute disponibilité est cochée dans la configuration du groupe de redondance de présence, procédez Uncheck avant le redémarrage du service. La configuration du groupe de redondance de présence est accessible à l'adresse CUCM Pub Administration > System > Presence Redundancy Group. Un redémarrage du service entraîne une interruption temporaire de la messagerie instantanée/du protocole et doit être effectué en dehors des heures de production.

· Connectez-vous à Cisco Unified Serviceability de l'éditeur :

a. Cisco Unified Serviceability > Tools > Control Center - Network Services.

b. Restart le service du routeur Cisco XCP.

c. Une fois le redémarrage du service terminé, continuez avec le serviceRestart de routeur Cisco XCP sur les abonnés.

Certificat CUP-XMPP-S2S

Étape 1. Ouvrez une interface utilisateur graphique pour chaque serveur de votre cluster. Commencez par l'éditeur IM/P, puis ouvrez une interface utilisateur graphique pour chaque serveur d'abonnés IM/P à tour de rôle et accédez à Cisco Unified OS Administration > Security > Certificate Management.

Étape 2. Commencez par l'interface utilisateur graphique de l'éditeur, choisissez Find d'afficher tous les certificats, puis sélectionnez le certificat àcup-xmpp-s2s.pem utiliser. Une fois ouvert, choisissez Regenerate et attendez que la fenêtre contextuelle soit fermée pour voir si le message a réussi.

Étape 3. Continuez avec les abonnés suivants et reportez-vous à la même procédure à l'étape 2, et terminez pour tous les abonnés de votre cluster.

Étape 4. Une fois que le certificat CUP-XMPP-S2S a été régénéré sur tous les noeuds, les services doivent être redémarrés dans l'ordre mentionné.

 **Remarque** : si la case Activer la haute disponibilité est cochée dans la configuration du groupe de redondance de présence, Uncheck procédez comme suit avant le redémarrage de ces services. La configuration du groupe de redondance de présence est accessible sur CUCM Pub Administration > System > Presence Redundancy Group. Un redémarrage des services entraîne une interruption temporaire de la messagerie instantanée et doit être effectué en dehors des heures de production.

· Connectez-vous à Cisco Unified Serviceability de l'éditeur :

a. Cisco Unified Serviceability > Tools > Control Center - Network Services.

b. Restart le service du routeur Cisco XCP.

c. Une fois le redémarrage du service terminé, continuez avec Restart du service de routeur Cisco XCP sur les abonnés.

· Connectez-vous à Cisco Unified Serviceability de l'éditeur :

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart le service Cisco XCP XMPP Federation Connection Manager.

c. Une fois le redémarrage du service terminé, continuez avec Restart du service Cisco XCP XMPP Federation Connection Manager sur les abonnés.

Certificat IPSec

 **Remarque** : le ipsec.pem certificat de l'éditeur CUCM doit être valide et présent dans tous les abonnés (noeuds CUCM et IM/P) du magasin de confiance IPSec. Le ipsec.pem certificat de l'abonné n'est pas présent dans l'éditeur en tant que magasin de confiance IPSec dans un déploiement standard. Afin de vérifier la validité, comparez les numéros de série dans le ipsec.pem certificat de CUCM-PUB avec l'approbation IPSec dans les abonnés. Ils doivent correspondre.



Remarque : le DRS utilise une communication SSL (Secure Socket Layer) entre l'agent source et l'agent local pour l'authentification et le cryptage des données entre les noeuds de cluster CUCM (noeuds CUCM et IM/P). DRS utilise les certificats IPsec pour son cryptage de clé publique/privée. Sachez que si vous supprimez le fichier (hostname.pem) de magasin d'approbations IPSEC de la page Certificate Management, DRS ne fonctionne pas comme prévu. Si vous supprimez manuellement le fichier d'approbation IPSEC, vous devez vous assurer que vous téléchargez le certificat IPSEC vers le magasin d'approbation IPSEC. Pour plus d'informations, reportez-vous à la page d'aide relative à la gestion des certificats dans les Guides de sécurité CUCM.

Étape 1. Ouvrez une interface utilisateur graphique pour chaque serveur de votre cluster. Commencez par l'éditeur IM/P, puis ouvrez une interface utilisateur graphique pour chaque serveur d'abonnés IM/P à tour de rôle et accédez à Cisco Unified OS Administration > Security > Certificate Management.

Étape 2. Commencez par l'interface utilisateur graphique de l'éditeur et choisissez Find d'afficher tous les certificats. Choisissez le certificat ipsec.pem. Une fois ouvert, choisissez Regenerate et attendez que la fenêtre contextuelle soit fermée pour voir si le message a réussi.

Étape 3. Continuez avec les abonnés suivants et reportez-vous à la même procédure à l'étape 2, et terminez pour tous les abonnés de votre cluster.

Étape 4. Une fois que tous les noeuds ont régénéré le certificat IPSEC, ces services sont alors Restart disponibles. Accédez à Cisco Unified Serviceability de l'éditeur ; Cisco Unified Serviceability > Tools > Control Center - Network Services.

- a. Sélectionnez Restart le service principal Cisco DRF.
- b. Une fois le service redémarré, choisissez Restart le service local DRF Cisco sur l'éditeur, puis continuez avec Restart le service local DRF Cisco sur chaque abonné.

Certificat Tomcat



Remarque : étant donné que Jabber utilise les certificats de serveur CUCM Tomcat et IM/P Tomcat et CUP-XMPP pour valider les connexions pour les services Tomcat et CUP-XMPP, ces certificats CUCM et IM/P sont dans la plupart des cas signés CA. Supposons que le périphérique Jabber ne dispose pas de la racine et d'un certificat intermédiaire faisant partie du certificat Tomcat installé dans son magasin de certificats de confiance. Dans ce cas, le client Jabber affiche une fenêtre contextuelle d'avertissement de sécurité pour le certificat non approuvé. S'il n'est pas déjà installé dans le magasin de certificats de confiance du périphérique Jabber, la racine et tout certificat intermédiaire doivent être envoyés au périphérique Jabber via la stratégie de groupe, MDM, e-mail, etc., qui dépend du client Jabber.

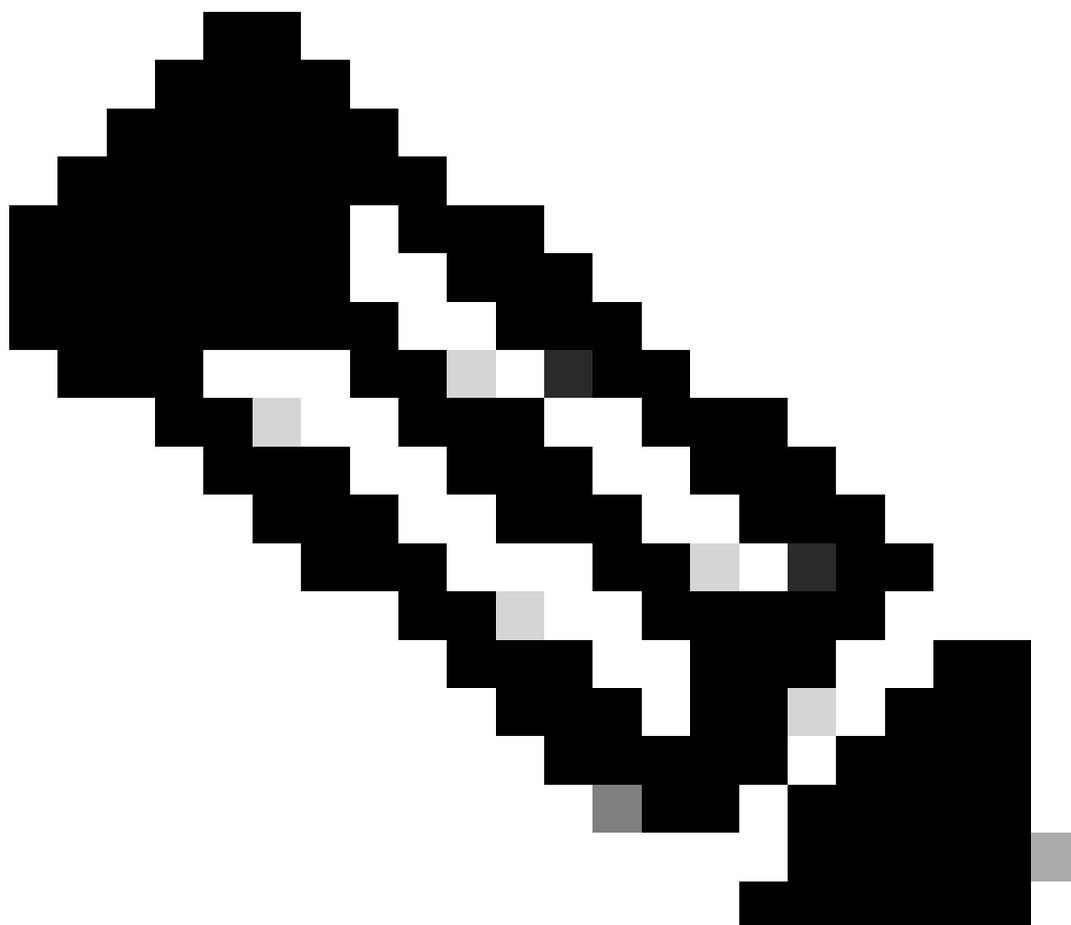


Remarque : si le certificat Tomcat est auto-signé, le client Jabber affiche une fenêtre contextuelle d'avertissement de sécurité pour le certificat non approuvé, si le certificat Tomcat n'est pas installé dans le magasin de certificats de confiance du périphérique Jabber. S'il n'est pas déjà installé dans le magasin de certificats de confiance du périphérique Jabber, le certificat auto-signé CUP-XMPP doit être envoyé au périphérique Jabber via la stratégie de groupe, MDM, e-mail, etc., qui dépend du client Jabber.

Étape 1. Ouvrez une interface utilisateur graphique pour chaque serveur de votre cluster. Commencez par l'éditeur IM/P, puis ouvrez successivement une interface utilisateur graphique pour chaque serveur d'abonnés IM/P et accédez à Cisco Unified OS Administration > Security > Certificate Management.

Étape 2. Commencez par l'interface utilisateur graphique de l'éditeur et choisissez Find d'afficher tous les certificats.
· Dans la colonne Type du certificat, tomcat.pem déterminez s'il est auto-signé ou signé par une autorité de certification.

tomcat.pem · Si le certificat est un multi-SAN de distribution signé par un tiers (type signé par une autorité de certification), consultez ce lien pour savoir comment générer un CSR Tomcat multi-SAN et le soumettre à l'autorité de certification pour un certificat Tomcat signé par une autorité de certification. [Exemple de configuration de cluster de communications unifiées avec un objet multi-serveur signé par une autorité de certification. Autre nom de configuration](#)



Remarque : le CSR Tomcat multi-SAN est généré sur l'éditeur CUCM et est distribué à tous les noeuds CUCM et IM/P du cluster.

· Si le tomcat.pem certificat est un noeud unique de distribution signé par un tiers (type signé par une autorité de certification) (le nom de distribution est le nom commun du certificat), consultez ce lien pour générer un CSR CUP-XMPP à noeud unique et envoyez-le à l'autorité de certification pour le certificat CUP-XMPP signé par une autorité de certification, [Guide pratique complet de Jabber pour la validation du certificat](#)

· Si le tomcat.pem certificat est auto-signé, passez à l'étape 3

Étape 3. Choisissez Find afin d'afficher tous les certificats :

- Sélectionnez le certificat de votre tomcat.pem choix.
- Une fois ouverte, choisissez Regenerate et attendez que la fenêtre contextuelle de réussite s'affiche avant de la fermer.

Étape 4. Continuez avec chaque abonné suivant, reportez-vous à la procédure de l'étape 2 et terminez tous les abonnés de votre cluster.

Étape 5. Une fois que tous les noeuds ont régénéré le certificat Tomcat, Restart le service Tomcat est activé sur tous les noeuds. Commencez par l'éditeur, puis par les abonnés.

- Pour Restart activer le service Tomcat, vous devez ouvrir une session CLI pour chaque noeud et exécuter la commande jusqu'à ce que le service redémarre Cisco Tomcat, comme illustré dans l'image :

```
admin:
admin:utils service restart Cisco Tomcat
Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat{STOPPING}
Cisco Tomcat{STOPPING}
Cisco Tomcat{STARTING}
Cisco Tomcat{STARTING}
Cisco Tomcat{STARTED}
admin: █
```

Supprimer les certificats de confiance expirés



Remarque : les certificats de confiance (qui se terminent par -trust) peuvent être supprimés le cas échéant. Les certificats de confiance qui peuvent être supprimés sont ceux qui ne sont plus nécessaires, ont expiré ou sont obsolètes. Ne supprimez pas les cinq certificats d'identité : les cup.pem , cup-xmpp.pem , cup-xmpp-s2s.pem , ipsec.pem , et les tomcat.pem certificats. Les redémarrages du service, comme illustré, sont conçus pour effacer toute information en mémoire de ces certificats hérités dans ces services.



Remarque : si la case Activer la haute disponibilité est cochée dans la configuration du groupe de redondance de présence, procédez Uncheck avant qu'un service ne soit Stopped/Started ou Restarted. La configuration du groupe de redondance de présence est accessible à l'adresse CUCM Pub Administration > System > Presence Redundancy Group. Un redémarrage de certains services, comme illustré, entraîne une interruption temporaire de la messagerie instantanée/instantanée et doit être effectué en dehors des heures de production.

Étape 1. Naviguez jusqu'à l'adresse :Cisco Unified Serviceability > Tools > Control Center - Network Services

- Dans le menu déroulant, choisissez votre éditeur IM/P, choisissez Stop dans Cisco Certificate Expiry Monitor, puis Stop dans Cisco Intercluster Sync Agent.

- Répétez Stop pour ces services pour chaque noeud IM/P de votre grappe.



Remarque : si le certificat Tomcat-trust doit être supprimé, accédez à Cisco Unified Serviceability > Tools > Control Center - Network Services de l'éditeur CUCM.

-
- Dans la liste déroulante, sélectionnez l'éditeur CUCM.
 - Faites votre choix Stop dans Cisco Certificate Expiry Monitor, puis Stop dans Cisco Certificate Change Notification.
 - Répétez l' pour chaque noeud CUCM de votre cluster.

Étape 2. Accédez à Cisco Unified OS Administration > Security > Certificate Management > Find.

- Recherchez les certificats de confiance expirés (pour les versions 10.x et ultérieures, vous pouvez filtrer par Expiration. Dans les versions antérieures à 10.0, vous devez identifier les certificats spécifiques manuellement ou via les alertes RTMT (si elles sont reçues).
- Le même certificat de confiance peut apparaître dans plusieurs noeuds, il doit être supprimé individuellement de chaque noeud.

- Choisissez le certificat de confiance à supprimer (selon la version, vous obtenez une fenêtre contextuelle ou vous êtes dirigé vers le certificat sur la même page).
- Choisissez Delete (vous obtenez une fenêtre contextuelle qui commence par « vous êtes sur le point de supprimer définitivement ce certificat... »).
- Cliquez sur OK.

Étape 3. Répétez le processus pour chaque certificat d'approbation à supprimer.

Étape 4. Une fois terminé, les services directement liés aux certificats supprimés doivent être redémarrés.

- CUP-trust : Cisco SIP Proxy, Cisco Presence Engine et, s'il est configuré pour SIP Federation, Cisco XCP SIP Federation Connection Manager (voir la section Certificat CUP)
- CUP-XMPP-trust : routeur Cisco XCP (voir la section relative au certificat CUP-XMPP)
- CUP-XMPP-S2S-trust : routeur Cisco XCP et gestionnaire de connexion de fédération Cisco XCP XMPP
- IPSec-trust : DRF Source/DRF Local (voir la section Certificat IPSec)
- Tomcat-trust : redémarrez le service Tomcat via la ligne de commande (voir la section Certificat Tomcat)

Étape 5. Redémarrez les services arrêtés à l'étape 1.

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

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.