Régénération des certificats pour CUCM

Contenu

Introduction

Ce document décrit la procédure de régénération des certificats dans Cisco Unified Communications Manager (CUCM) version 8.X et ultérieure.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- *Outil de surveillance en temps réel* (RTMT)
- Certificats CUCM

Components Used

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

- CUCM version 8.X et ultérieure

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

Ce document décrit la procédure pas à pas sur la façon de régénérer des certificats dans Cisco Unified Communications Manager (CUCM) version 8.X et ultérieure. Cependant, cela ne reflète pas les changements postérieurs à la version 12.0 à la récupération ITL.

Installer RTMT

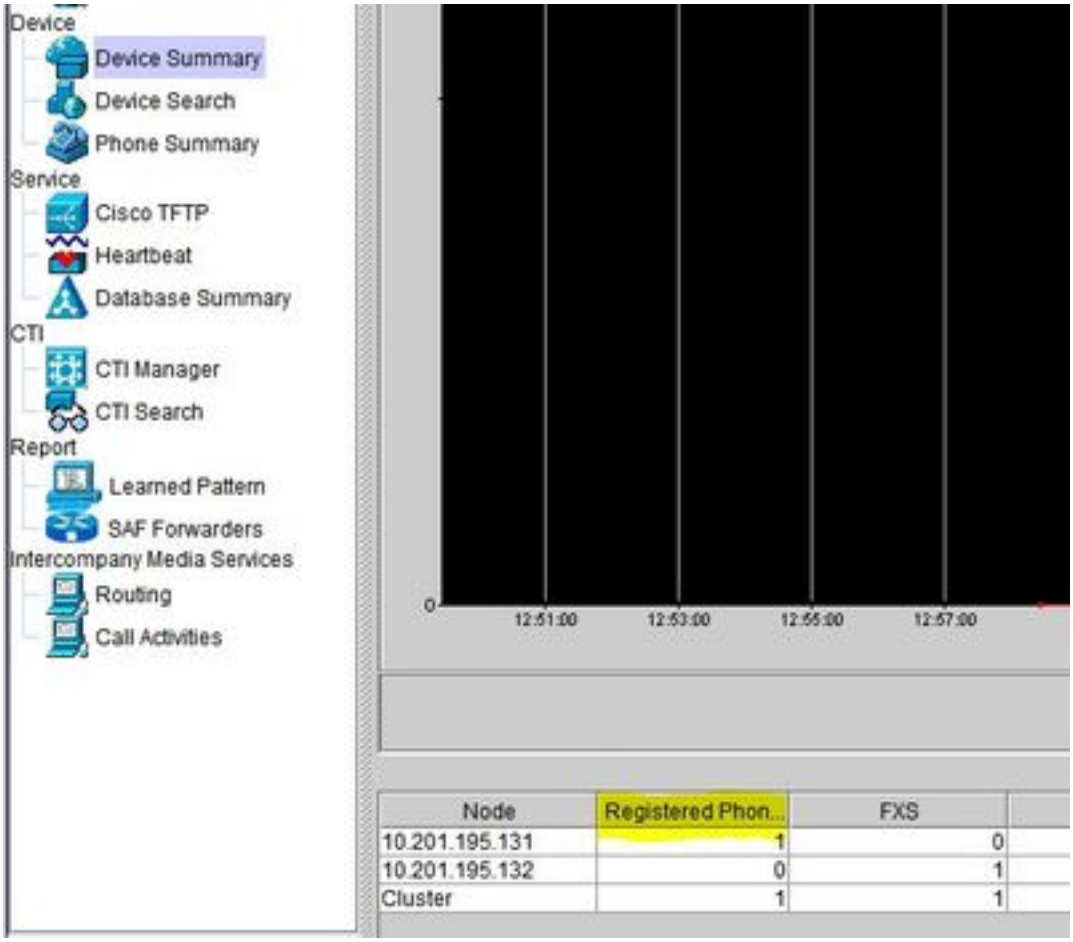
- Téléchargez et installez l'outil RTMT depuis Call Manager. Accédez à Call Manager (CM) Administration : **Application > Plugins > Rechercher > Outil de surveillance en temps réel Cisco Unified - Windows > Télécharger** Installation et lancement

Surveillance des terminaux avec RTMT

- Lancez RTMT et entrez l'adresse IP ou le nom de domaine complet (FQDN), puis le nom d'utilisateur et le mot de passe pour accéder à l'outil :
- Sélectionnez l'**onglet Voix/Vidéo**.Sélectionnez **Device Summary**. Cette section indique le nombre total de terminaux enregistrés et le nombre de terminaux connectés à chaque noeudSurveiller pendant la réinitialisation du terminal pour garantir l'enregistrement avant la régénération du certificat suivant

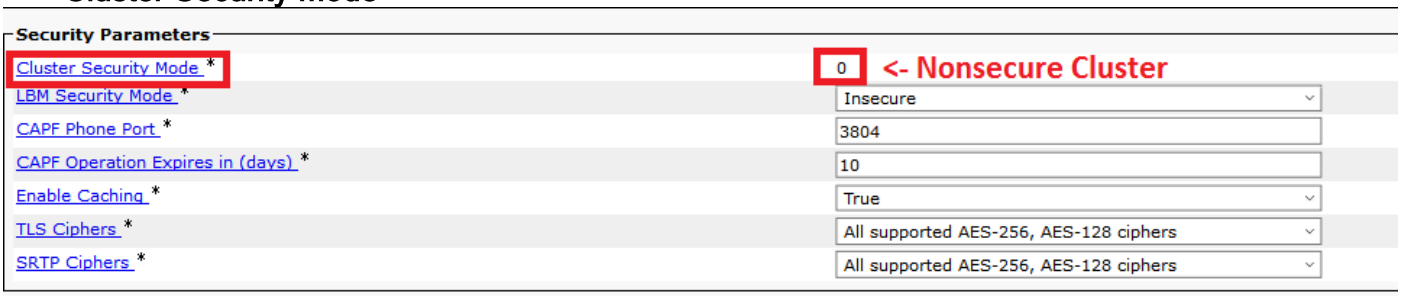
Astuce : Le processus de régénération de certains certificats peut avoir un impact sur le terminal. Envisagez un plan d'action après les heures normales de bureau en raison de la nécessité de redémarrer les services et les téléphones. Vérifiez que l'enregistrement du téléphone via RTMT est fortement recommandé.

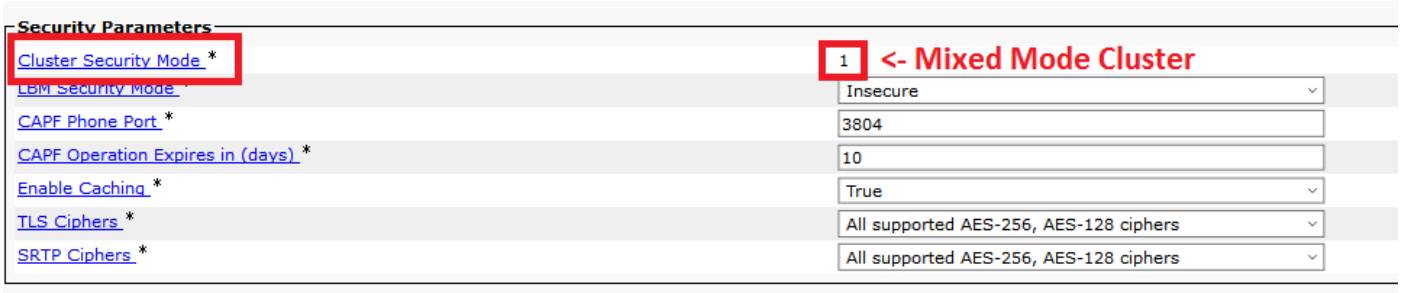
Avertissement : Les points de terminaison présentant une incompatibilité ITL peuvent rencontrer des problèmes d'enregistrement après ce processus. La suppression de l'ITL sur le terminal est une solution typique des meilleures pratiques une fois le processus de régénération terminé et tous les autres téléphones enregistrés.



Déterminez si votre cluster est en mode mixte ou non sécurisé

- Accédez à CM Administration. **System > Enterprise Parameters > Security Parameters > Cluster Security Mode**





Impact par le magasin de certificats

Pour que le système fonctionne correctement, il est essentiel que tous les certificats soient mis à jour dans le cluster CUCM. Si les certificats sont expirés ou non valides, ils peuvent affecter considérablement le fonctionnement normal du système. L'impact peut varier selon la

configuration de votre système. Une liste de services pour les certificats spécifiques qui ne sont pas valides ou ont expiré est affichée ici :

CallManager.pem

- Les téléphones cryptés/authentifiés ne s’enregistrent pas
- Le protocole TFTP (Trivial File Transfer Protocol) n'est pas approuvé (les téléphones n'acceptent pas les fichiers de configuration signés et/ou les fichiers ITL)
- Les services téléphoniques peuvent être affectés
- Les liaisons SIP (Secure Session Initiation Protocol) ou les ressources multimédias (ponts de conférence, point de terminaison multimédia (MTP), codeurs XC, etc.) ne s'enregistrent pas et ne fonctionnent pas.
- La requête AXL échoue.

Tomcat.pem

- Les téléphones ne peuvent pas accéder aux services HTTP hébergés sur le nœud CUCM, tels que l’annuaire d’entreprise
- CUCM peut présenter divers problèmes Web, tels que l'impossibilité d'accéder aux pages de service d'autres noeuds du cluster
- Problèmes de mobilité des postes (EM) ou de mobilité des postes entre clusters
- Authentification unique (SSO)
- Si UCCX (Unified Contact Center Express) est intégré, en raison d'un changement de sécurité par rapport à CCX 12.5, il est nécessaire d'avoir téléchargé le certificat Tomcat de CUCM (auto-signé) ou le certificat racine et intermédiaire de Tomcat (pour CA signé) dans le magasin UCCX tomcat-trust, car cela affecte les connexions de bureau Finesse.

CAPF.pem

- Les téléphones ne s'authentifient pas pour le VPN téléphonique, 802.1x ou le proxy téléphonique
- Impossible d'émettre des certificats LSC (Locally Significative Certificate) pour les téléphones.
- Les fichiers de configuration chiffrés ne fonctionnent pas

IPSec.pem

- Le système de reprise après sinistre (DRS)/le cadre de reprise après sinistre (DRF) ne peut pas fonctionner correctement
- Les tunnels IPsec vers d’autres grappes CUCM ne fonctionnent pas

TVS (Trust Verification Service)

Le service de vérification de la confiance (TVS) est le principal composant de la sécurité par défaut. TVS permet aux téléphones IP Cisco Unified d'authentifier les serveurs d'applications, tels que les services EM, le répertoire et MIDlet, lorsque HTTPS est établi.

TVS offre les fonctionnalités suivantes :

- Évolutivité : les ressources du téléphone IP Cisco Unified ne sont pas affectées par le nombre de certificats de confiance.
- Flexibilité : l'ajout ou la suppression de certificats de confiance sont automatiquement répercutés dans le système.
- Sécurité par défaut : les fonctions de sécurité des signaux et autres que les supports font partie de l'installation par défaut et ne nécessitent aucune intervention de l'utilisateur.

ITL et CTL

- ITL contient le rôle de certificat pour Call Manager TFTP, tous les certificats TVS dans le cluster et la fonction de proxy d'autorité de certification (CAPF) lors de l'exécution.
- CTL contient des entrées pour les services SAST (System Administrator Security Token), Cisco CallManager et Cisco TFTP exécutés sur le même serveur, CAPF, serveur(s) TFTP et pare-feu ASA (Adaptive Security Appliance). TVS n'est pas référencé dans CTL.

Processus de régénération de certificat

> **Note**: Tous les terminaux doivent être mis sous tension et enregistrés avant la régénération des certificats. Sinon, les téléphones non connectés nécessitent le retrait de l'ITL.

Certificat Tomcat

Identifiez si des certificats tiers sont utilisés :

1. Accédez à chaque serveur de votre cluster (dans des onglets distincts de votre navigateur Web) en commençant par l'éditeur, puis par chaque abonné. Accédez à **Cisco Unified OS Administration > Security > Certificate Management > Find**.
   Observez à partir de la colonne Description si Tomcat indique un certificat auto-signé généré par le système. Si Tomcat est signé par un tiers, suivez le lien fourni et effectuez ces étapes après la régénération de Tomcat.Certificats tiers signés, reportez-vous à Téléchargement CUCM de certificats CCMAdmin Web GUI.
2. Sélectionnez **Find** afin d'afficher tous les certificats : Sélectionnez le certificat **Tomcat pem**.Une fois ouvert, sélectionnez **Regenerate** et attendez que vous voyiez la fenêtre contextuelle Success, puis fermez la fenêtre contextuelle ou revenez en arrière et sélectionnez **Find/List**.
3. Continuez avec chaque Abonné suivant, suivez la même procédure à l'étape 2 et effectuez sur tous les Abonnés de votre cluster.
4. Une fois que tous les noeuds ont régénéré le certificat Tomcat, redémarrez le service Tomcat sur tous les noeuds. Commencez par l'éditeur, puis par les abonnés. Pour redémarrer Tomcat, vous devez ouvrir une session CLI pour chaque noeud et exécuter la commande **utils service restart Cisco Tomcat**.

5. Ces étapes sont nécessaires dans l'environnement CCX, le cas échéant :

- Si un certificat auto-signé est utilisé, téléchargez les certificats Tomcat à partir de tous les noeuds du cluster CUCM vers le magasin de confiance Tomcat Unified CCX.
- Si un certificat CA signé ou un certificat CA signé privé est utilisé, téléchargez le certificat CA racine de CUCM vers le magasin de confiance Tomcat Unified CCX.
- Redémarrez les serveurs comme indiqué dans le document de régénération de certificat pour CCX.

Références supplémentaires :

- Guide de gestion des certificats de la solution UCCX
- Utilitaire de vérification du fonctionnement Unified CCX

Certificat IPSEC

Note: CUCM/IM&P (Instant Messaging and Presence) avant la version 10.X du DRF Master L'agent s'exécute sur CUCM Publisher et IM&P Publisher. Le service local DRF s'exécute respectivement sur les abonnés. Versions 10.X et ultérieures, DRF Master L'agent s'exécute sur le serveur de publication CUCM uniquement et le service local DRF sur les abonnés CUCM et IM&P Publisher et les abonnés.

Note: Le système de reprise après sinistre utilise une communication SSL (Secure Socket Layer) entre les Master Agent et agent local pour l'authentification et le chiffrement des données entre les noeuds de cluster CUCM. DRS utilise les certificats IPSec pour son cryptage de clé publique/privée. Notez que si vous supprimez le fichier IPSEC truststore (hostname.pem) de la page Certificate Management, les DRS ne fonctionnent pas comme prévu. Si vous supprimez manuellement le fichier de confiance IPSEC, vous devez vous assurer que vous téléchargez le certificat IPSEC vers le magasin de confiance IPSEC. Pour plus de détails, reportez-vous à la page d'aide relative à la gestion des certificats dans les guides de sécurité de Cisco Unified Communications Manager.

1. Accédez à chaque serveur de votre cluster (dans des onglets distincts de votre navigateur Web) en commençant par l'éditeur, puis par chaque abonné. Accédez à **Cisco Unified OS Administration > Security > Certificate Management > Find**:
   Sélectionnez le certificat **IPSEC pem**.Une fois ouvert, sélectionnez **Regenerate** et attendez que vous voyiez la fenêtre contextuelle Success, puis fermez la fenêtre contextuelle ou revenez en arrière et sélectionnez **Find/List**.
2. Continuer avec les abonnés suivants ; suivez la même procédure à l'étape 1 et effectuez l'opération sur tous les abonnés de votre cluster.
3. Une fois que tous les noeuds ont régénéré le certificat IPSEC, redémarrez les services. Accédez à Publisher **Cisco Unified Serviceability**. **Cisco Unified Serviceability > Outils > Control Center - Services réseau**.Sélectionnez **Redémarrer** le **DRF Cisco** Masterservice.Une

fois le redémarrage du service terminé, sélectionnez **Restart** sur le **service local Cisco DRF** sur l'éditeur, puis continuez avec les abonnés et sélectionnez **Restart** sur le **service local Cisco DRF**.

Le certificat IPSEC.pem dans l'éditeur doit être valide et doit être présent dans tous les abonnés en tant que magasins de confiance IPSEC. Le certificat IPSEC.pem des abonnés ne peut pas être 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 certificat IPSEC.pem du PUB avec la confiance IPSEC dans les SUB. Ils doivent correspondre.

Certificat CAPF

Avertissement : Vérifiez que vous avez identifié si votre cluster est en mode mixte avant de continuer. Reportez-vous à la section **Identifier si votre cluster est en mode mixte ou non sécurisé**.

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. Voir Token et liens sans jeton.
2. Accédez à chaque serveur de votre cluster (dans des onglets distincts de votre navigateur Web), en commençant par l'éditeur, puis par chaque abonné. Accédez à **Cisco Unified OS Administration > Security > Certificate Management > Find**. Sélectionnez le certificat **CAPF pem**.Une fois ouvert, sélectionnez **Regenerate** et attendez que vous voyiez la fenêtre contextuelle Success, puis fermez la fenêtre contextuelle ou revenez en arrière et sélectionnez **Find/List**
3. Continuer avec les abonnés suivants ; suivez la même procédure à l'étape 2 et effectuez l'opération sur tous les abonnés de votre cluster. Si le cluster est en mode mixte UNIQUEMENT et que le CAPF a été régénéré, mettez à jour la CTL avant de continuer Token - Tokenless.Si le cluster est en mode mixte, le service Call Manager doit également être redémarré avant le redémarrage des autres services.
4. Une fois que tous les noeuds ont régénéré le certificat CAPF, redémarrez les services. Accédez à Publisher **Cisco Unified Serviceability**. **Cisco Unified Serviceability > Outils > Control Center - Services de fonctionnalités**.Commencez par l'éditeur et sélectionnez **Redémarrer** sur le **service de fonction proxy de l'autorité de certification Cisco** uniquement lorsque cette option est active.
5. Accédez à **Cisco Unified Serviceability > Tools > Control Center - Network Services**. Commencez par l'éditeur, puis continuez avec les abonnés, sélectionnez **Restart** on **Cisco Trust Verification Service**. Accédez à **Cisco Unified Serviceability > Tools > Control Center - Feature Services**.Commencez par l'éditeur, puis continuez avec les abonnés et redémarrez le **service Cisco TFTP** uniquement lorsqu'il est actif.
6. Redémarrer tous les téléphones : **Administration de Cisco Unified CM > Système > Paramètres d'entreprise**Sélectionnez **Reset** puis une fenêtre contextuelle s'affiche avec l'instruction **You are about to reset all devices in the system. Cette action ne peut pas être annulée. Continuer ?,** sélectionnez **OK** puis **Réinitialiser**.

Les téléphones sont maintenant réinitialisés. Surveillez leurs actions via l'outil RTMT pour vous assurer que la réinitialisation a réussi et que les périphériques se réenregistrent auprès de CUCM. Attendez la fin de l'enregistrement du téléphone avant de passer au certificat suivant. Ce

processus d'enregistrement des téléphones peut prendre un certain temps. Attention, les périphériques qui avaient des ITL défectueux avant le processus de régénération ne sont pas réenregistrés dans le cluster tant qu'il n'a pas été supprimé.

Certificat CallManager

> **Avertissement :** Vérifiez que vous avez identifié si votre cluster est en mode mixte avant de continuer. Reportez-vous à la section **Identifier si votre cluster est en mode mixte ou non sécurisé**.

> **Avertissement :** Ne régénérez pas les certificats CallManager.PEM et TVS.PEM en même temps. Cela entraîne une non-correspondance irrécupérable avec l'ITL installé sur les points d'extrémité qui nécessitent la suppression de l'ITL de TOUS les points d'extrémité du cluster. Terminez le processus complet pour CallManager.PEM et, une fois les téléphones réenregistrés, démarrez le processus pour TVS.PEM.

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. Voir Token et liens sans jeton.
2. Accédez à chaque serveur de votre cluster (dans des onglets distincts de votre navigateur Web), en commençant par l'éditeur, puis par chaque abonné. Accédez à **Cisco Unified OS Administration > Security > Certificate Management > Find**.
   Sélectionnez le certificat pem CallManager.Une fois ouvert, sélectionnez **Regenerate** et attendez que vous voyiez la fenêtre contextuelle Success, puis fermez la fenêtre contextuelle ou revenez en arrière et sélectionnez **Find/List**.
3. Continuer avec les abonnés suivants ; suivez la même procédure à l'étape 2 et effectuez l'opération sur tous les abonnés de votre cluster. Si le cluster est en mode mixte UNIQUEMENT et que le certificat CallManager a été régénéré, mettez à jour la CTL avant de poursuivre Token - Tokenless
4. Connectez-vous à Publisher Cisco Unified Serviceability : Accédez à **Cisco Unified Serviceability > Tools > Control Center - Feature Services**.Commencez par l'éditeur, puis continuez avec les abonnés, puis redémarrez le **service Cisco CallManager** s'il est actif.
5. Accédez à **Cisco Unified Serviceability > Tools > Control Center - Feature Services** Commencez par l'éditeur, puis continuez avec les abonnés et redémarrez le **service Cisco TIManager** uniquement lorsqu'il est actif.
6. Accédez à **Cisco Unified Serviceability > Tools > Control Center - Network Services**. Commencez par le logiciel de publication, puis continuez avec les abonnés et redémarrez **Cisco Trust Verification Service**.
7. Accédez à **Cisco Unified Serviceability > Tools > Control Center - Feature Services**. Commencez par le serveur de publication, puis continuez avec les abonnés et redémarrez le **service Cisco TFTP** uniquement lorsqu'il est actif.
8. Redémarrer tous les téléphones : **Administration de Cisco Unified CM > Système > Paramètres d'entreprise**Sélectionnez **Reset** puis une fenêtre contextuelle s'affiche avec l'instruction **You are about to reset all devices in the system. Cette action ne peut pas être annulée. Continuer ?,** sélectionnez **OK** puis **Réinitialiser**

Les téléphones sont maintenant réinitialisés. Surveillez leurs actions via l'outil RTMT pour vous assurer que la réinitialisation a réussi et que les périphériques se réenregistrent auprès de CUCM. Attendez la fin de l'enregistrement du téléphone avant de passer au certificat suivant. Ce processus d'enregistrement des téléphones peut prendre un certain temps. Notez que les périphériques qui avaient des ITL défectueux avant le processus de régénération ne se réenregistrent pas dans le cluster tant que l'ITL n'est pas supprimé.

Certificat TVS

> **Avertissement :** Ne régénérez pas les certificats CallManager.PEM et TVS.PEM en même temps. Cela entraîne une non-correspondance irrécupérable avec l'ITL installé sur les points d'extrémité qui nécessitent la suppression de l'ITL de TOUS les points d'extrémité du cluster.

> **Note**: TVS authentifie les certificats pour le compte de Call Manager. Régénérez ce certificat en dernier.

Accédez à chaque serveur de votre cluster (dans des onglets distincts de votre navigateur Web), en commençant par l'éditeur, puis par chaque abonné. Accédez à **Cisco Unified OS Administration > Security > Certificate Management > Find**:

- Sélectionnez le certificat **pem TVS**.
- Une fois ouvert, sélectionnez **Regenerate** et attendez que vous voyiez la fenêtre contextuelle Success, puis fermez la fenêtre contextuelle ou revenez en arrière et sélectionnez **Find/List**.

1. Continuer avec les abonnés suivants ; suivez la même procédure à l'étape 1 et effectuez l'opération sur tous les abonnés de votre cluster. Une fois que tous les noeuds ont régénéré le certificat TVS, redémarrez les services : Connectez-vous à Publisher **Cisco Unified Serviceability**. Accédez à **Cisco Unified Serviceability > Tools > Control Center - Network Services**.Sur l'éditeur, sélectionnez **Restart** on **Cisco Trust Verification Service**.Une fois le redémarrage du service terminé, poursuivez avec les abonnés et redémarrez le service de **vérification de la confiance Cisco**.
2. Commencez par le logiciel de publication, puis continuez avec les abonnés et redémarrez le **service Cisco TFTP** uniquement lorsqu'il est actif.
3. Redémarrer tous les téléphones : **Administration de Cisco Unified CM > Système > Paramètres d'entreprise**.Sélectionnez **Reset** puis une fenêtre contextuelle s'affiche avec l'instruction **You are about to reset all devices in the system. Cette action ne peut pas être annulée. Continuer ?,** sélectionnez **OK** puis **Réinitialiser**.

Les téléphones sont maintenant réinitialisés. Surveillez leurs actions via l'outil RTMT pour vous assurer que la réinitialisation a réussi et que les périphériques se réenregistrent auprès de CUCM. Attendez la fin de l'enregistrement du téléphone avant de passer au certificat suivant. Ce processus d'enregistrement des téléphones peut prendre un certain temps. Notez que les périphériques qui avaient des ITL défectueux avant le processus de régénération ne se réenregistrent pas dans le cluster tant que l'ITL n'est pas supprimé.

Certificat de récupération ITLR

> **Note**: Le certificat de récupération ITLR est utilisé lorsque les périphériques perdent leur état

de confiance. Le certificat apparaît à la fois dans l'ITL et la CTL (lorsque le fournisseur CTL est actif).
Si des périphériques perdent leur état d'approbation, vous pouvez utiliser la commande **utils itl reset localkey** pour les clusters non sécurisés et la commande **utils ctl reset localkey** pour les clusters en mode mixte. Lisez le guide de sécurité de votre version Call Manager pour vous familiariser avec la façon dont le certificat ITLRecovery est utilisé et le processus requis pour récupérer l'état de confiance.
Si le cluster a été mis à niveau vers une version qui prend en charge une longueur de clé de 2048 et que les certificats de serveur de clusters ont été régénérés vers 2048 et que l'ITLRecovery n'a pas été régénéré et a actuellement une longueur de clé de 1024, la commande de récupération ITL échoue et la méthode ITLRecovery n'est pas utilisée.

1. Accédez à chaque serveur de votre cluster (dans des onglets distincts de votre navigateur Web), en commençant par l'éditeur, puis par chaque abonné. Accédez à **Cisco Unified OS Administration > Security > Certificate Management > Find**:
Sélectionnez le certificat **pem de récupération ITLRecovery**.Une fois ouvert, sélectionnez **Regenerate** et attendez que vous voyiez la fenêtre contextuelle Success, puis fermez la fenêtre contextuelle ou revenez en arrière et sélectionnez **Find/List**.
2. Continuer avec les abonnés suivants ; suivez la même procédure à l'étape 2 et effectuez l'opération sur tous les abonnés de votre cluster.
3. Une fois que tous les noeuds ont régénéré le certificat ITLRecovery, les services doivent être redémarrés dans l'ordre suivant : Si vous êtes en mode mixte - Mettez à jour la CTL avant de continuer Token - Tokenless.Connectez-vous à Publisher **Cisco Unified Serviceability**.
Accédez à **Cisco Unified Serviceability > Tools > Control Center - Network Services**.Sur l'éditeur, sélectionnez **Restart** on **Cisco Trust Verification Service**. Une fois le redémarrage du service terminé, poursuivez avec les abonnés et redémarrez le service de **vérification de la confiance Cisco**.
4. Commencez par le logiciel de publication, puis continuez avec les abonnés et redémarrez le **service Cisco TFTP** uniquement lorsqu'il est actif.
5. Redémarrer tous les téléphones : **Administration de Cisco Unified CM > Système > Paramètres d'entreprise**Sélectionnez **Reset** puis une fenêtre contextuelle s'affiche avec l'instruction **You are about to reset all devices in the system. Cette action ne peut pas être annulée. Continuer ?,** sélectionnez **OK** puis **Réinitialiser**.
6. Les téléphones téléchargent maintenant la nouvelle ITL/CTL pendant leur réinitialisation.

Supprimer les certificats de confiance expirés

Note: Identifiez les certificats de confiance qui doivent être supprimés, qui ne sont plus nécessaires ou qui ont expiré. Ne supprimez pas les cinq certificats de base qui incluent CallManager.pem, tomcat.pem, ipsec.pem, CAPF.pem et TVS.pem. Les certificats de confiance peuvent être supprimés le cas échéant. Le service suivant qui redémarre est conçu pour effacer les informations des certificats hérités dans ces services.

1. Accédez à **Cisco Unified Serviceability > Tools > Control Center - Network Services**. Dans la liste déroulante, sélectionnez le serveur de publication CUCM.Sélectionnez **Arrêter la notification de modification de certificat**.Répétez l' pour chaque noeud Call Manager de votre cluster.Si vous disposez d'un serveur IMP : Dans le menu déroulant, sélectionnez vos serveurs IMP un par un et sélectionnez **Arrêter l'administration de la plate-forme, les services**

Web et l'agent Cisco Intercluster Sync.

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. Pour les versions inférieures 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.Sélectionnez le certificat de confiance à supprimer (selon votre version, vous obtenez une fenêtre contextuelle ou vous avez accédé au certificat sur la même page) Sélectionnez **Supprimer**. (Vous obtenez une fenêtre contextuelle qui commence par « vous êtes sur le point de supprimer définitivement ce certificat ».*)*Sélectionnez **OK**.
3. Répétez le processus pour chaque certificat de confiance à supprimer.
4. Une fois l'opération terminée, vous devez redémarrer les services directement liés aux certificats supprimés. Vous n'avez pas besoin de redémarrer les téléphones dans cette section. Call Manager et CAPF peuvent avoir un impact sur les terminaux. Tomcat-trust : redémarrer le service Tomcat via la ligne de commande (voir la section Tomcat)CAPF-trust : redémarrez la fonction proxy de Cisco Certificate Authority (voir la section CAPF) Ne redémarrez pas les terminaux.CallManager-trust : Service CallManager/CTIManager (voir la section CallManager) Ne redémarrez pas les terminaux. Affecte les terminaux et provoque les redémarrages.Confiance IPSEC : DRF Master/DRF Local (voir la section IPSEC).TVS (Self-Signed) ne dispose pas de certificats de confiance.
5. Redémarrez les services précédemment arrêtés à l'étape 1.

Vérification

Les procédures de vérification ne sont pas disponibles pour cette configuration.

Dépannage

Les procédures de dépannage ne sont pas disponibles 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.