Régénérer Les Certificats Dans Unified Communications Manager

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Installer l'outil de surveillance en temps réel (RTMT)
  - Surveillance des terminaux avec RTMT
  - Identifier le mode de sécurité du cluster
    - ITL et CTL
  - Impact par le magasin de certificats
    - CallManager.pem/CallManager-ECDSA.pem
    - Tomcat.pem/Tomcat-ECDSA.pem
    - CAPF.pem
    - IPSec.pem
    - Service de vérification de la confiance (TVS)
- Processus de régénération de certificat
  - Certificat Tomcat
  - Certificat IPSEC
  - Certificat CAPF
  - Certificat CallManager
  - Certificat TVS
  - Certificat de récupération ITLR
- Supprimer les certificats de confiance expirés
- Vérification
- Dépannage

Introduction

Ce document décrit les procédures de régénération des certificats dans Unified Communications Manager, les effets et les conditions requises pour réussir.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Outil de surveillance en temps réel (RTMT)
- Guide de sécurité pour Cisco Unified Communications Manager
- Certificats CUCM
- Mode Mixte
- Fonction Proxy De L'Autorité De Certification

Composants utilisés

Cisco recommande d'installer les outils suivants :

- Outil de surveillance en temps réel (RTMT)
- Informations basées sur les versions 15.0+ de Cisco Unified Communications Manager (CUCM).

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 15.X et ultérieure. Reportez-vous au guide de sécurité correspondant à votre version spécifique.

Les versions héritées qui sont en fin de vie ne sont pas prises en compte.

Communications Manager (CUCM) version 12.0+ l'ITL est signé par le certificat de récupération ITLR.

Communications Manager (CUCM) version 12.0+ en mode mixte, la CTL est signée par le certificat de récupération ITLR.

Le mode mixte est un mode qui active des fonctions de sécurité améliorées tout en maintenant la compatibilité avec les terminaux hérités ou non sécurisés.

Le téléphone IP Cisco s'appuie sur le fichier CTL pour connaître le mode de sécurité du cluster (mode non sécurisé ou mixte). Le fichier CTL effectue le suivi du mode de sécurité du cluster en

incluant le certificat Unified Communications Manager dans l'enregistrement Unified Communications Manager. La CTL est générée uniquement après que le cluster a été placé en mode mixte.

Le fichier ITL contient également l'indication du mode de sécurité du cluster.

Certificat d'identité : Certificat qui représente l'identité d'un utilisateur ou d'un périphérique (application/serveur). Il contient la clé publique de l'autorité de certification qui a émis le certificat et inclut des informations telles que les détails du propriétaire du certificat et la période de validité du certificat.



Comparaison des signataires ITL

Installer l'outil de surveillance en temps réel (RTMT)

- Téléchargez et installez l'outil RTMT depuis Call Manager.
    - Accédez à Call Manager (CM) Administration : Application > Plugins > Rechercher > Cisco Unified Real-Time Monitoring Tool - Windows > Télécharger. Installation et lancement.

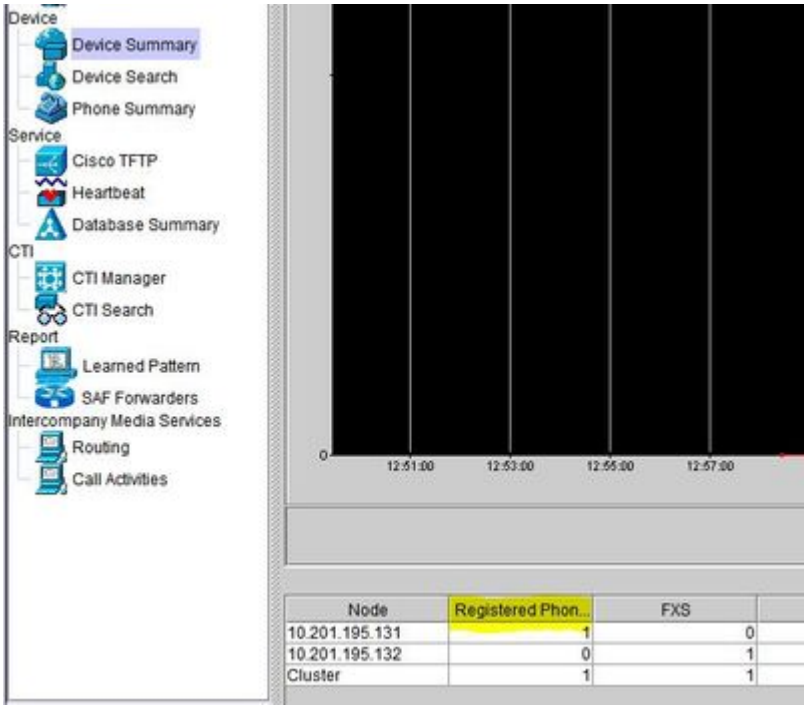
Surveillance des terminaux avec RTMT

- 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 noeud.
        - Surveillez pendant la réinitialisation du point d'extrémité pour vous assurer de l'enregistrement avant la régénération du certificat suivant.

Conseil : Le processus de régénération de certains certificats peut avoir un impact sur les

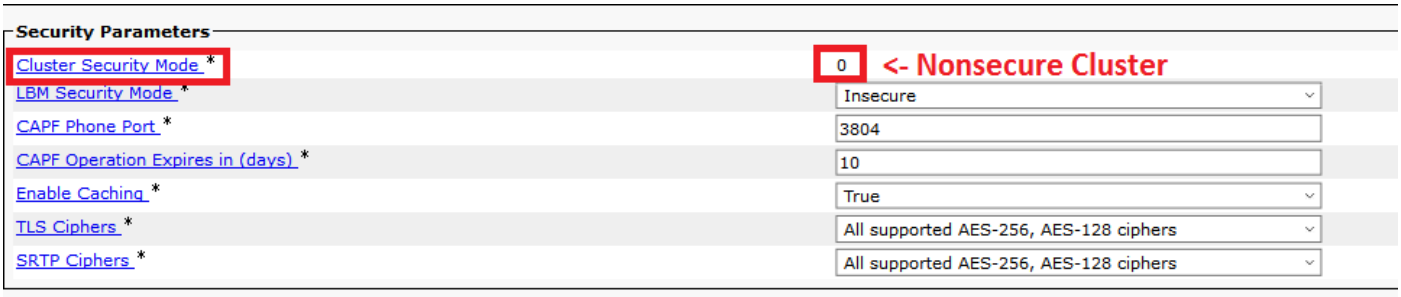
terminaux. Envisagez un plan d'action après les heures normales de bureau en raison de la nécessité de redémarrer les services et les téléphones. Il est vivement recommandé de vérifier l'enregistrement du téléphone via RTMT avant, pendant et après le processus. Vous ne devez redémarrer les services que s'ils sont en cours d'exécution sur le serveur.

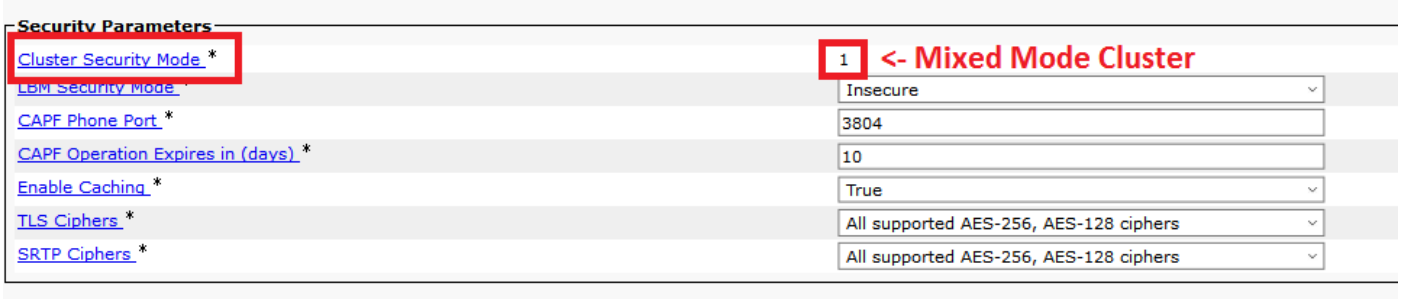
Avertissement : Les points de terminaison qui présentent actuellement une non-correspondance ITL (ITL incorrect) peuvent rencontrer des problèmes d'enregistrement après ce processus. Pour les périphériques dont l'ITL est défectueux, la suppression de l'ITL sur le terminal est une solution de meilleure pratique typique une fois le processus de régénération terminé et tous les autres téléphones enregistrés. Vérifiez les modèles de téléphone spécifiques pour savoir comment supprimer les certificats ITL/CTL (sécurité).



Identifier le mode de sécurité du cluster

- Accédez à CM Administration : Système > Paramètres d'entreprise > Paramètres de sécurité > Mode de sécurité du cluster.





ITL et CTL

- La liste de confiance initiale (ITL) contient le rôle de certificat pour Call Manager TFTP, ITLRecovery et tous les certificats TVS dans le cluster. Il peut également contenir la fonction proxy de l'autorité de certification (CAPF) si le service est en cours d'exécution. À partir de la version 12.0, l'ITL est signé par le certificat ITLRecovery. Vous pouvez le voir en vous connectant à l'interface de ligne de commande et en entrant la commande show itl. Avant la version 12.0, l'ITL était signé par le certificat Call Manager.
- CTL contient des entrées pour les services System Administrator Security Token (SAST), Cisco CallManager et Cisco TFTP exécutés sur le même serveur, CAPF, ITLRecovery, serveur(s) TFTP et pare-feu ASA (Adaptive Security Appliance). TVS n'est pas référencé dans CTL. La CTL est fournie aux terminaux si le service, Cisco CTL Provider, est en cours d'exécution.
- À partir de CUCM 14SU(3), le service Cisco CTL Provider ne prend plus en charge les jetons CTL et Tokenless est la méthode prise en charge par défaut.

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 de manière significative le fonctionnement normal du système. L'impact peut varier en fonction de la configuration de votre système. Voici les services pour les certificats spécifiques qui ne sont pas valides ou ont expiré :

CallManager.pem/CallManager-ECDSA.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 (enregistrement automatique, substitution de poste, intergrappe de substitution de poste)
- Les liaisons SIP (Secure Session Initiation Protocol) ou les ressources multimédias (SIP TLS, ponts de conférence, Media Termination Point (MTP), codeurs XC, etc., Exp-C TLS

Traversal Zone) ne s'enregistrent pas et ne fonctionnent pas.
- La requête AXL échoue.

Tomcat.pem/Tomcat-ECDSA.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 à partir d'autres noeuds du cluster.
- Problèmes de mobilité des postes (EM) ou de mobilité des postes entre clusters.
- Reprise après sinistre
- Authentification unique (SSO)
- Expressway Traversal Zone down (TLS Verify est activé).
- Si Unified Contact Center Express (UCCX) 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 Tomcat (pour CA signé) dans le magasin UCCX tomcat-trust, car cela affecte les connexions de bureau Finesse.

CAPF.pem

- Ce certificat est utilisé pour émettre des LSC vers les points d'extrémité (sauf en mode CAPF en ligne et hors ligne), Phone VPN, 802.1x, Phone Proxy, Application User CAPF Profiles.
- À partir de la version 11.5(1) SU1 d'Unified Communications Manager, tous les certificats LSC émis par le service CAPF sont signés avec l'algorithme SHA-256.
- Configuration de l'authentification et du chiffrement pour CTI, JTAPI et TAPI.

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 la passerelle (GW) ou vers d'autres clusters CUCM ne fonctionnent pas.

Service de vérification de la confiance (TVS)

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.
- Demandes de service téléphonique et validation par vérification de certificat.

ITLRecovery (Service de vérification de la confiance)

- 8.X - 11.5 Récupération des téléphones avec ITL inadapté, migration du téléphone et EMCC vers CUCM 12.0+.
- 12.0+ Utilisé dans SSO, EMCC et signataire principal de ITL/CTL.
- La récupération ITL 12.5+ est uniquement générée par le serveur de publication

Support ECDSA du gestionnaire de certificats

Dans Unified Communications Manager version 11.0, le gestionnaire de certificats prend en charge à la fois la génération de certificats ECDSA auto-signés et la demande de signature de certificat ECDSA (CSR). Les versions antérieures d'Unified Communications Manager prenaient uniquement en charge le certificat RSA. Cependant, à partir de la version 11.0 d'Unified Communications Manager, le certificat CallManager-ECDSA a été ajouté avec le certificat RSA existant.

Les certificats CallManager et CallManager-ECDSA partagent le même magasin de certificats de confiance : CallManager-Trust. Unified Communications Manager télécharge ces certificats dans ce magasin d'approbations.

Certificat d'identité signé par une autorité de certification tierce

---

Remarque : Tiers peut signifier l'autorité de certification interne (CA) ou des sources externes comme Go-Daddy, Verisign, et d'autres. Le certificat d'identité est le certificat du serveur pour le rôle spécifique (Tomcat, Call Manager, etc.). Les certificats signés auront au moins une autorité de certification racine qui a signé le certificat d'identité. Dans la plupart des cas, un intermédiaire ou des multiples. Le chemin du certificat peut ressembler à : Racine - Intermédiaire - Certificat d'identité.

---

1. Accédez à chaque serveur de votre cluster (dans des onglets distincts de votre navigateur Web, sauf si vous créez un CSR multi-SAN) en commençant par l'éditeur, suivi de chaque

abonné. Accédez à Cisco Unified OS Administration > Security > Certificate Management.
2. Sélectionnez Generate CSR (produire CSR).
3. Sélectionnez la liste déroulante Fonction du certificat et sélectionnez le certificat.
4. Sélectionnez le type de distribution. Serveur unique ou multiserveur (SAN).
    - Le réseau multiserveur (SAN) inclut tous les noeuds CUCM et CUP dans la section SAN.
5. Sélectionnez Générer.
6. Téléchargez le CSR et fournissez-le à votre autorité de certification.
7. Après avoir reçu le certificat signé, téléchargez les certificats par ordre de chaîne.
    - Téléchargez le ROOT en tant que certificat de confiance.
    - Téléchargez le certificat intermédiaire en tant que certificat d'approbation.
    - Téléchargez le certificat signé comme type de certificat.
    - Redémarrez les services appropriés identifiés dans la fenêtre contextuelle.

Processus de régénération de certificat

Remarque : 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

Le processus de régénération de Tomcat et de Tomcat-ECDSA est identique, y compris les redémarrages de service.

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 en suivant chaque abonné. Naviguez jusqu'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, utilisez le lien fourni et exécutez ces étapes après la régénération de Tomcat.
    - Certificats signés par des tiers, reportez-vous à Téléchargement CUCM des certificats de l'interface graphique Web CCMAdmin.
2. Sélectionnez Rechercher pour afficher tous les certificats :
    - Sélectionnez l'option Find Tomcat Pem.
    - Une fois ouvert, sélectionnez Regenerate et attendez que vous voyez la fenêtre contextuelle Success, puis fermez la fenêtre contextuelle ou revenez en arrière et sélectionnez Find/List.
3. Continuez avec chaque Abonné suivant, effectuez 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 et continuez avec les abonnés.
    - Pour redémarrer Tomcat, vous devez ouvrir une session CLI pour chaque noeud et exécuter la commande utils service restart Cisco Tomcat.
    - Si votre cluster est configuré pour SSO, ou à l'aide d'OAuth, vous devez redémarrer le service SSOSP avec utils service restart Cisco SSOSP Tomcat.

```
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:
```

5. Ces étapes sont utilisées à partir de l'environnement CCX, le cas échéant :

- Si un certificat auto-signé est utilisé, téléchargez les certificats Tomcat de tous les noeuds du cluster CUCM vers le magasin d'approbation Tomcat de 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 de 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

Remarque : CUCM/IM&P (Instant Messaging and Presence) avant la version 10.X, l'agent maître DRF s'exécute sur CUCM Publisher et IM&P Publisher. Le service local DRF s'exécute respectivement sur les abonnés. Versions 10.X et ultérieures, l'agent maître DRF 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.

Remarque : Le système de reprise après sinistre utilise une communication SSL (Secure Socket Layer) entre l'agent maître et l'agent local pour l'authentification et le cryptage des données entre les noeuds de cluster CUCM. DRS utilise les certificats IPSec pour son cryptage de clé publique/privée. Sachez que si vous supprimez le fichier IPSEC truststore

(hostname.pem) de la page Certificate Management, DRS ne fonctionne 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 d'informations, 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) et commencez par l'éditeur, suivi de chaque abonné. Naviguez jusqu'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. Poursuivre avec les abonnés suivants ; effectuez la même procédure à l'étape 1 et effectuez-la 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.
        1. Cisco Unified Serviceability > Tools > Control Center - Network Services.
        2. Sélectionnez Redémarrer sur le service principal Cisco DRF.
        3. 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.
        4. Redémarrez le service tomcat sur tous les noeuds. Commencez par l'éditeur et continuez avec les abonnés.
            - Pour redémarrer Tomcat, vous devez ouvrir une session CLI pour chaque noeud et exécuter la commande utils service restart Cisco Tomcat.

Certificat CAPF

Remarque : À partir de CUCM 14, le certificat CAPF se trouve uniquement sur l'éditeur.

Avertissement : Assurez-vous d'avoir identifié si votre cluster est en mode mixte avant de continuer. Reportez-vous à la section Identifier le mode de sécurité du cluster.

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. S'il est 1, alors le cluster est en mode mixte et vous devez mettre à jour le fichier CTL après la mise à jour du certificat et avant le redémarrage des services.
2. Accédez au serveur Publisher dans votre cluster Accédez à Cisco Unified OS Administration > Security > Certificate Management > Find.
    - Sélectionnez le certificat PEM CAPF.

- 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.
- Si le cluster est en mode mixte ou si la CTL est utilisée pour 802.1X, vous devez mettre à jour la CTL avant de continuer.
    - Connectez-vous à l'interface de ligne de commande du serveur de publication et entrez la commande utils ctl update CTLFile.
    - Réinitialisez tous les téléphones chiffrés et authentifiés pour que la mise à jour du fichier CTL prenne effet.

3. Une fois que le serveur de publication a régénéré le certificat CAPF, redémarrez les services.
    - Accédez à Publisher Cisco Unified Serviceability.
        1. Cisco Unified Serviceability > Outils > Control Center - Services de fonctionnalités.
        2. Sélectionnez l'éditeur et sélectionnez Redémarrer sur le service de fonction proxy de l'autorité de certification Cisco, uniquement si actif.
4. Accédez à Cisco Unified Serviceability > Tools > Control Center - Network Services.
    - Commencez par l'éditeur, puis continuez avec les abonnés et 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, redémarrez Cisco TFTP Service où l'état affiche Started.
5. Redémarrer tous les téléphones :
    - Option 1 - 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.
        - Cette méthode réinitialise TOUS les composants du Gestionnaire d'appels.
    - Option 2 - Cisco Unified CM Administration > Bulk Administration > Phones > Update Phones >Query
        - La recherche du nom du périphérique commence par SEP > Next > Reset Phones > Run Immediate.

Les téléphones sont maintenant réinitialisés. Surveillez leurs actions via l'outil RTMT pour vous assurer que la réinitialisation a réussi et que les périphériques sont réenregistrés dans 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 CallManager

Le processus de régénération de CallManager et de CallManager-ECDSA est identique, y compris les redémarrages de service.

⚠ Avertissement : Assurez-vous d'avoir identifié si votre cluster est en mode mixte avant de continuer. Reportez-vous à la section Identifier le mode de sécurité du cluster.

⚠ Avertissement : Ne régénérez pas les certificats CallManager.PEM et TVS.PEM en même temps dans les versions 8.x-11.5, ou si l'ITL est signé par le certificat Call Manager. 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 dans le cluster, ou la restauration à partir de DRS pour recommencer les mises à jour de certificat.

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. S'il est 1, alors 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. Naviguez jusqu'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. Poursuivre avec les abonnés suivants ; effectuez la même procédure à l'étape 2 et effectuez-la sur tous les abonnés de votre cluster.
    - Si le cluster est en mode mixte ou si la CTL est utilisée pour 802.1X, vous devez mettre à jour la CTL avant de continuer.
        - Connectez-vous à l'interface de ligne de commande du serveur de publication et entrez la commande utils ctl update CTLFile.
        - Réinitialisez tous les téléphones chiffrés et authentifiés pour que la mise à jour du fichier CTL prenne effet.
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, redémarrez uniquement le service Cisco CallManager où l'état affiche Démarré.
5. 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 TIManager où l'état affiche Démarré.
6. Accédez à Cisco Unified Serviceability > Tools > Control Center - Network Services.
    - Commencez par le serveur 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 où l'état affiche Démarré.
8. Si votre cluster est configuré pour utiliser SSO ou OAuth, vous devez redémarrer le service Cisco HAProxy.

- Afin de redémarrer Tomcat SSOSP, vous devez ouvrir une session CLI pour chaque noeud et exécuter la commande utils service restart Cisco HAProxy.

9. Redémarrer tous les téléphones :
    - Option 1 - 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.
        - Cette méthode réinitialise TOUS les composants du Gestionnaire d'appels.
    - Option 2 - Cisco Unified CM Administration > Bulk Administration > Phones > Update Phones > Query
        - La recherche du nom du périphérique commence par SEP > Next > Reset Phones > Run Immediately

Les téléphones sont maintenant réinitialisés. Surveillez leurs actions via l'outil RTMT pour vous assurer que la réinitialisation a réussi et que les périphériques sont réenregistrés dans 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 dans les versions 8.x-11.5, ou si l'ITL est signé par le certificat Call Manager. 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 dans le cluster, ou la restauration à partir de DRS pour recommencer les mises à jour de certificat.

Remarque : 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. Naviguez jusqu'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. Poursuivre avec les abonnés suivants ; effectuez la même procédure à l'étape 1 et effectuez-la 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 serveur de publication, puis continuez avec les abonnés, redémarrez le service Cisco TFTP Service où l'état affiche Démarré.
3. Redémarrer tous les téléphones :
   - Option 1 - 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.
     - Cette méthode réinitialise TOUS les composants du Gestionnaire d'appels.
   - Option 2 - Cisco Unified CM Administration > Bulk Administration<s/trong> > Phones<s/trong> > Update Phones > Query
     - La recherche du nom du périphérique commence par SEP > Next > Reset Phones > Run Immediate.

Les téléphones sont maintenant réinitialisés. Surveillez leurs actions via l'outil RTMT pour vous assurer que la réinitialisation a réussi et que les périphériques sont réenregistrés dans 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

Remarque : 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 dans la CTL (lorsque le fournisseur de CTL est actif, ID de bogue Cisco CSCwf85275).
À partir de la version 12.5+, ITLRecovery est un certificat unique généré par l'éditeur et distribué aux abonnés.
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. Naviguez jusqu'à Publisher Cisco Unified OS Administration > Security > Certificate Management > Find.
    - Sélectionnez le certificat pem de récupération ITLRecovery.
    - Une fois ouvert, sélectionnez Regenerate et attendez que la fenêtre contextuelle Success s'affiche, puis fermez la fenêtre contextuelle ou revenez en arrière et sélectionnez Find/List.
2. Une fois que ITLRecovery a été régénéré dans le certificat ITLRecovery, les services doivent être redémarrés.
    - Si le cluster est en mode mixte ou si la CTL est utilisée pour 802.1X, vous devez mettre à jour la CTL avant de continuer.
        - Connectez-vous à l'interface de ligne de commande du serveur de publication et entrez la commande utils ctl update CTLFile.
    - 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.
3. Commencez par le serveur de publication, puis continuez avec les abonnés, redémarrez le service Cisco TFTP Service où l'état affiche Démarré.
4. Redémarrer tous les téléphones :
    - Option 1 - 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.
        - Cette méthode réinitialise TOUS les composants du Gestionnaire d'appels.
    - Option 2 - Cisco Unified CM Administration > Bulk Administration > Phones > Update Phones >Query
        - La recherche du nom du périphérique commence par SEP > Next > Reset Phones > Run Immediate.

Supprimer les certificats de confiance expirés

Avertissement : La suppression d'un certificat peut affecter le fonctionnement de votre système. Il peut également rompre une chaîne de certificats si le certificat fait partie d'une chaîne existante. Vérifiez cette relation à partir du nom d'utilisateur et du nom de sujet des certificats concernés dans la fenêtre Liste de certificats.

Remarque : Un certificat approuvé est le seul type de certificat que vous pouvez supprimer. Vous ne pouvez pas supprimer un certificat auto-signé généré par votre système. 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 l'éditeur CUCM.
        - Pour CUCM 11.5 et versions antérieures,
        - Sélectionnez Arrêter la notification de modification de certificat. Cette exigence n'est pas nécessaire pour CUCM version 12.0 et ultérieure.
        - 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. Cette exigence n’est pas nécessaire pour IMP version 12.0 et ultérieure.
2. Naviguez jusqu'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 antérieures à 10.0, identifiez manuellement les certificats ou utilisez 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 Delete (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 d'approbation à supprimer.
4. Une fois l'opération terminée, les services directement liés aux certificats supprimés doivent être redémarrés. 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 : redémarrez le service Tomcat via la ligne de commande (voir la section Tomcat).
    - CAPF-trust : redémarrez la fonction proxy de l'autorité de certification Cisco (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) n'a pas de certificats de confiance.
5. Redémarrez les services précédemment arrêtés à l'étape 1.

Vérification

Pour répertorier les certificats présents sur CUCM à partir de l'interface de ligne de commande, utilisez la sortie de commande suivante :

```
run sql select c.servername, tcs.name, dist.moniker, c.ipv4address, c.certificate from certificate as c
```

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.