Expiration et suppression de certificat de CallManager

Contenu

Introduction

Ce document décrit un problème avec le Cisco CallManager (cm) où vous recevez le **CertExpiryEmergency : Délivrez un certificat l'échéance** message d'alarme **EMERGENCY_ALARM du** client de l'outil de suivi en temps réel (RTMT), et offrez une solution au problème.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance des versions 6.x à 9.x cm, et que votre système :

- N'a pas une configuration de Système de noms de domaine (DNS). Ceci est fait pour la simplicité du document, mais beaucoup de systèmes l'ont configuré qui est CORRECT.
- A un certificat qui est expiré et doit être régénéré, ou un certificat qui est programmé pour expirer.

  Remarque: L'adresse IP du système n'importe pas si vous sélectionnez la **nouvelle** ou **régénérée** commande de **générer** après que vous changiez le nom d'hôte ou l'adresse IP.

Composants utilisés

Les informations dans ce document sont basées sur le serveur de Cisco cm avec des pages de gestion.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Problème

Vous recevez un **CertExpiryEmergency : Délivrez un certificat l'échéance** message d'alarme **EMERGENCY_ALARM du** RTMT en cm :

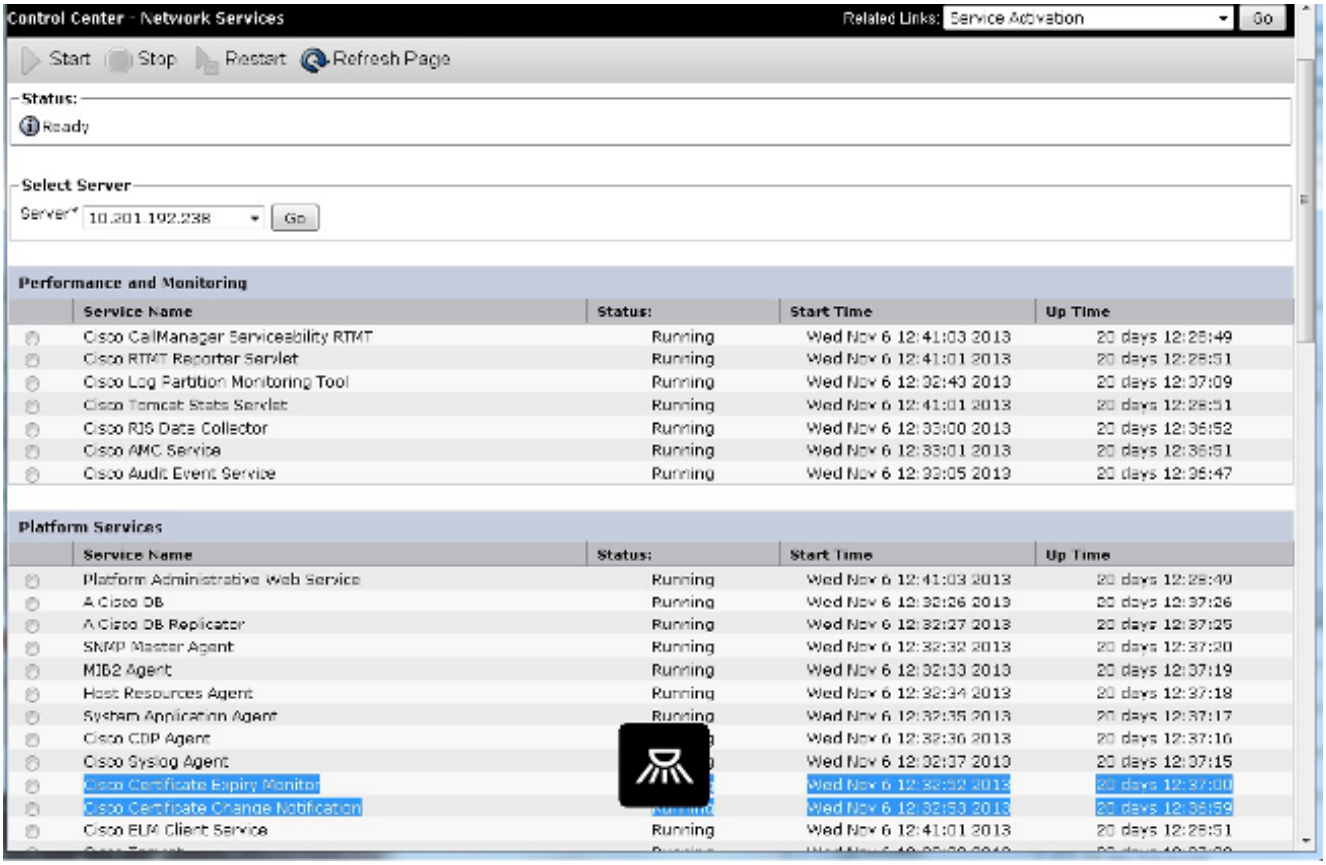
```
Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 629: Jul 30 17:00:00.352 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification.
 Certificate name:CAPF Unit:CAPF Type:own-cert
Expiration:Fri Dec 28 12:14:42:000 EST 2012 / App ID:Cisco Certificate
Monitor Cluster ID:Node ID:HOST-CM-PRI

Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 630: Jul 30 17:00:00.353 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification. Certificate name:CAPF-5d0a9888
Unit:CallManager-trust Type:trust-cert Expiration:Fri Dec 28 App ID:
 Cisco Certificate
Monitor Cluster ID: Node ID:HOST-CM-PRI

Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 631: Jul 30 17:00:00.354 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification. Certificate name:CAPF-5d0a9888
Unit:CAPF-trust Type:trust-cert Expiration:Fri Dec 28 12:14:4 App ID:
 Cisco Certificate
Monitor Cluster ID: Node ID:HOST-CM-PRI
```

Solution

Employez les informations dans cette section afin de résoudre le problème de message d'alarme cm.

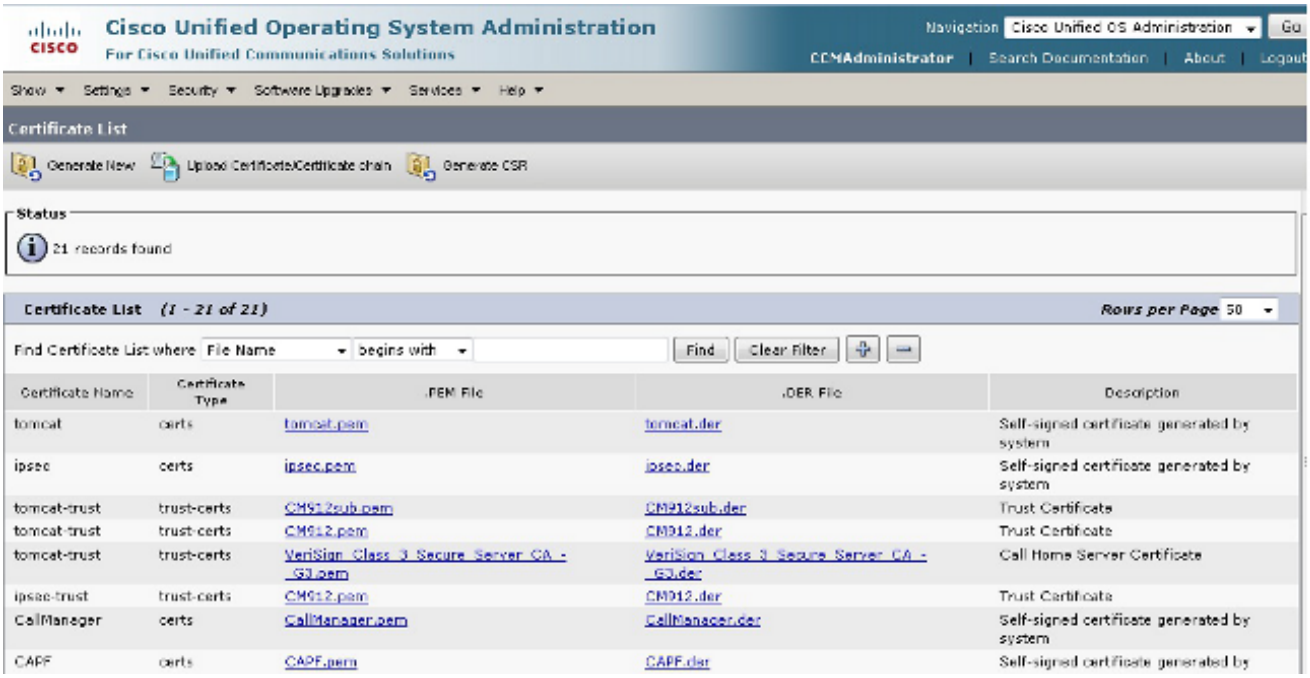
1. Du cm LE GUI unifié de page d'utilité, naviguent vers le **Tools > Control Center - des services réseau**.

2. Arrêtez l'**échéance moniteur de certificat de Cisco** et les **Services de notification de modification de certificat de Cisco** sur tous les serveurs dans la batterie :



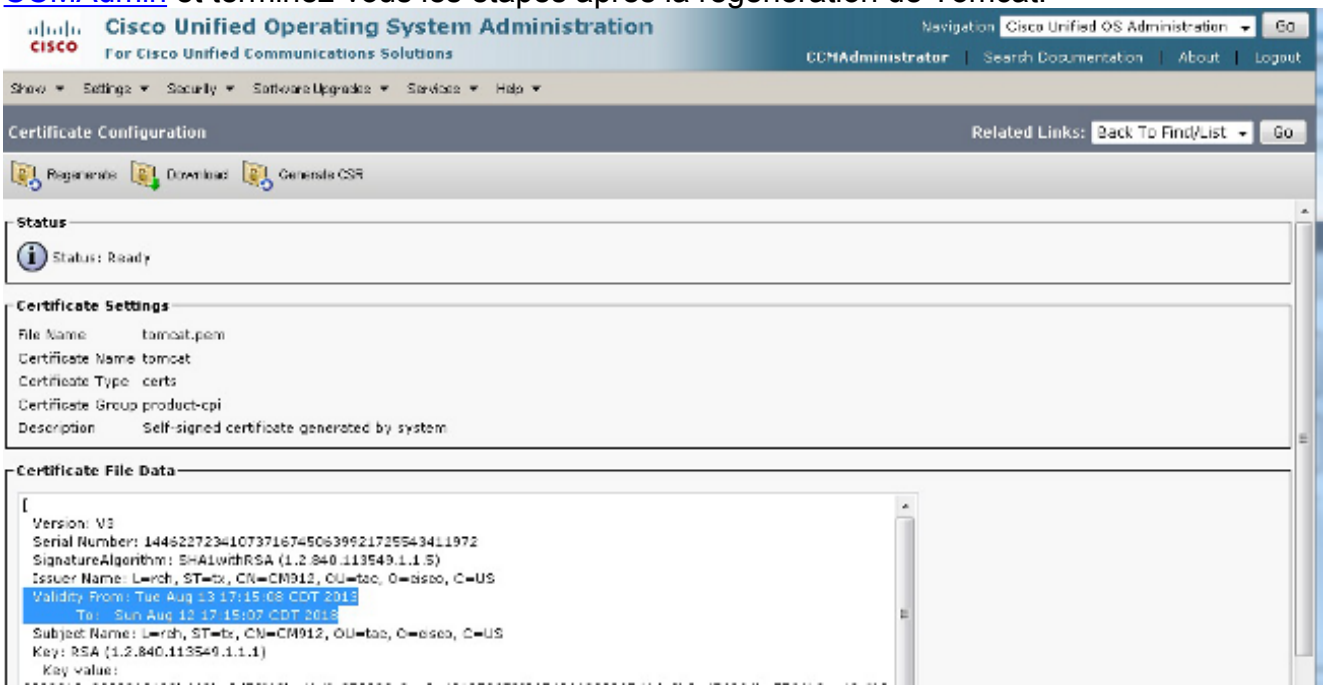
3. Du GUI du système d'exploitation de gestion (de SYSTÈME D'EXPLOITATION), naviguez vers la **Gestion de Sécurité > de certificat**, et ce des affichages de l'écran :

4. Cliquez sur Find afin d'afficher tous les Certificats sur un serveur particulier :

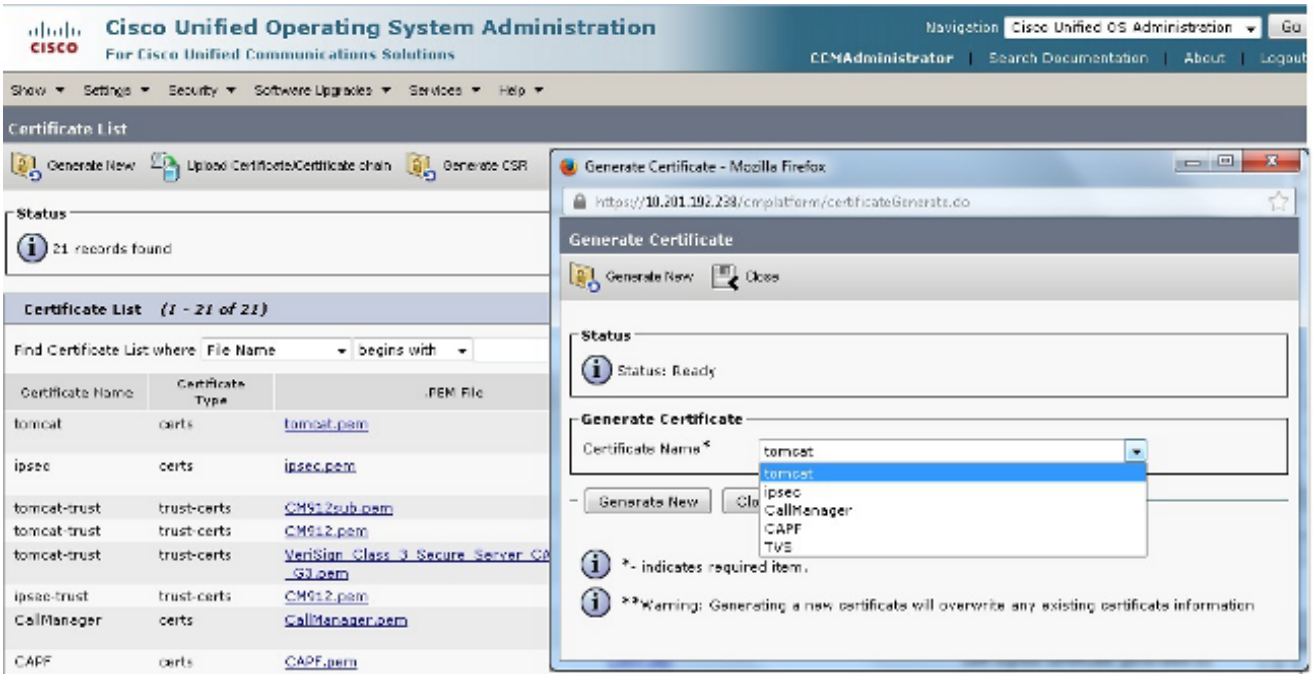


5. Cliquez sur n'importe quel certificat (un certificat de Tomcat dans ce cas) et visualisez la date, comme mis en valeur dans la prochaine image. Pour des Certificats de Tomcat, vérifiez si le serveur utilise un tiers certificat pour la procédure de connexion de page de **ccmadmin**. Vous pouvez vérifier ceci quand vous vous connectez dans la page d'un navigateur.

   Remarque: Si c'est un certificat signé de tierce partie, mettez en référence le CUCM téléchargeant l'article de la Communauté de support de Cisco de Certificats GUI de Web de CCMAdmin et terminez-vous les étapes après la régénération de Tomcat.

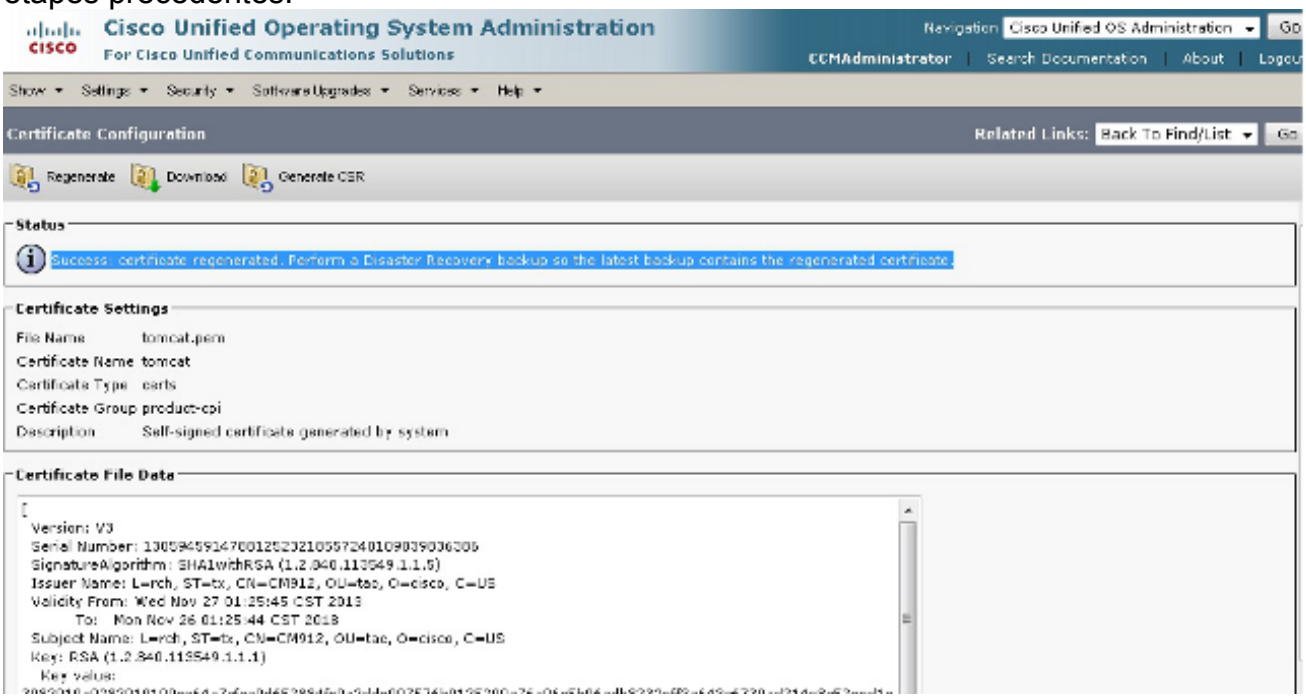


6. Naviguez vers la page de **Gestion de certificat** sur Publisher. Trouvez et cliquez sur le **fichier tomcat.pem**, et puis cliquez sur le régénéré **:**



7. Afin de redémarrer le service de Tomcat sur ce noeud, ouvrir un CLI au noeud et sélectionner la commande de **Cisco Tomcat de reprise de service d'utils**. Une fois le certificat est généré, un message s'affiche afin de confirmer que le certificat est en cours.

   Remarque: Le certificat est également vérifié par les informations de date décrites dans les étapes précédentes.



8. Complétez ce processus pour chacun des abonnés dans la batterie afin de régénérer les Certificats de chat.

Régénération de certificat pour des versions 8.x et ultérieures CUCM

Employez les informations dans cette section afin de régénérer les Certificats expirés pour des versions 8.x et ultérieures de Cisco Unified Communications Manager (CUCM).

Remarque: Régénérez les Certificats après des heures normales de bureau, parce que vous devez redémarrer des services et redémarrer les téléphones dans le processus.

CAPF

Pour la régénération de la fonction de proxy d'autorité de certification (CAPF), assurez-vous que la batterie n'est pas en mode sécurisé de batterie : naviguez vers le **System > Enterprise Parameters de la** page Web de gestion cm, et recherchez le **mode sécurisé de batterie**. Si la valeur est **0**, alors la batterie n'est pas en mode sécurisé de batterie. Si la valeur est tout nombre autres que zéro, alors la batterie est en mode sécurisé, et vous devez utiliser le client de la liste de confiance de certificat (CTL) afin de mettre le fichier CTL à jour.

Remarque: Mettez en référence le pour en savoir plus d'article de la Communauté du degré de sécurité de téléphone IP et de support CTL (liste de confiance de certificat) Cisco.

1. De Publisher, naviguez vers la page de Gestion de certificat.
2. Ouvrez le **fichier CAPF.pem** et cliquez sur le régénéré**. Ceci** renouvelle le certificat et crée deux nouveaux fichiers de confiance : on est la Cm-confiance et l'autre est la CAPF-confiance.
3. La de la page d'utilité, naviguez vers des **outils > des services de caractéristique**.
4. Si le service CAPF est lancé sous des **services de caractéristique**, alors redémarrez le service. Si le service CAPF n'est pas lancé, alors une reprise n'est pas nécessaire.
5. Naviguez vers des **outils > des services réseau de la** page d'utilité, et redémarrez le service du service de vérification de confiance (TV).
6. Naviguez vers des **outils > des services de caractéristique de la** page d'utilité, spécifiez le noeud, et redémarrez le service TFTP.
7. Une fois que les services sont redémarrés, redémarrez les téléphones de sorte qu'ils puissent récupérer le fichier mis à jour de la liste de confiance d'identité (ITL).
8. Revenez à la page de Gestion de certificat et supprimez les deux vieux fichiers de confiance. Ce sont les deux fichiers expirés de confiance que vous avez reçus de la sortie erreurs. Les nouveaux Certificats ont un numéro de série qui sélectionne le **fichier CAPF.pem**.
9. Terminez-vous les étapes précédentes pour chaque abonné.

IPSec

Les Certificats d'IPSec (IPSec) affectent le maître et les gens du pays de la panne de Reprise sur sinistre (DRF), qui traitent des fonctions de sauvegarde et de restauration.

1. Naviguez vers la page de gestion de SYSTÈME D'EXPLOITATION sur Publisher.

2. Naviguez vers la **Gestion de Sécurité > de certificat** et cliquez sur le **fichier IPSEC.pem**.

3. **Régénéré de** clic afin de mettre le dossier à jour de confiance.

4. Redémarrez le serveur que le certificat a été régénéré en fonction. Ceci est exigé parce que chaque service doit être redémarré après n'importe quelles régénération/mise à jour de n'importe quel certificat. Cependant, IPSec n'a pas une capacité de reprise de service autre que de redémarrer le noeud entier. Si d'autres Certificats doivent être mis à jour/régénérés, terminez-vous toutes les étapes et puis redémarrez le noeud après tout que les Certificats ont été traités. Ceci permet au serveur pour avoir tous les Certificats mis à jour dans le truststore et pour lire dedans correctement.

Cm

1. Naviguez vers la page de gestion de SYSTÈME D'EXPLOITATION sur Publisher.

2. Naviguez vers la page de Gestion de certificat, cliquez sur Find, cliquez sur le **fichier CallManager.pem**, et puis cliquez sur le régénéré**.**

3. Naviguez vers des **outils > le service de caractéristique à la** page d'utilité, trouvez le noeud spécifié, et redémarrez le service de Cisco cm.

4. De la page d'utilité, naviguez vers des **outils > des services réseau**, et redémarrez le service TV.

5. De la page d'utilité, naviguez vers des **outils > des services de caractéristique**, spécifiez le noeud, et redémarrez les services cm et CTI.

6. Redémarrez les téléphones de sorte qu'ils puissent récupérer le fichier mis à jour ITL.

7. Terminez-vous les étapes précédentes pour chaque abonné.

TV

1. Naviguez vers la page de gestion de SYSTÈME D'EXPLOITATION sur Publisher.

2. Naviguez vers la **Gestion de Sécurité > de certificat**, cliquez sur Find, cliquez sur le **fichier TVS.pem**, et puis cliquez sur le régénéré**.**

3. De la page d'utilité, naviguez vers des **outils > des services réseau**, et redémarrez le service TV.

4. De la page d'utilité, naviguez vers des **outils > des services de caractéristique**, spécifiez le noeud, et redémarrez le service TFTP.

5. Redémarrez les téléphones de sorte qu'ils puissent récupérer le fichier mis à jour ITL.

6. Terminez-vous les étapes précédentes pour chaque abonné.

Deletes certificates

Quand vous des deletes certificates, vous assurez que les services précédemment mentionnés sont arrêtés, et que les Certificats que vous supprimez ne sont pas actuellement utilisés ou sont expirés réellement.

En outre, vérifiez toujours toutes les informations dans le certificat, parce que vous ne pouvez pas le sauvegarder après suppression.