Activez la caractéristique de configuration chiffrée sur le CUCM

Contenu

Introduction

Ce document décrit l'utilisation des fichiers chiffrés de téléphone de configuration sur Cisco Unified Communications Manager (CUCM).

Informations générales

L'utilisation des fichiers de configuration chiffrés pour des téléphones est une fonctionnalité de sécurité facultative qui est disponible dans le CUCM.

Vous pas requis d'exécuter la batterie CUCM dans le mode mixte pour que cette caractéristique fonctionne correctement, car les informations de certificat de la fonction de proxy d'autorité de certification (CAPF) n'êtes sont contenues dans le fichier de la liste de confiance d'identité (ITL).

> **Note**: C'est l'emplacement par défaut pour toutes les versions 8.X et ultérieures CUCM. Pour des versions CUCM avant la version 8.X, vous devez s'assurer que les cluster run dans le mode mixte si vous désirez utiliser cette caractéristique.

Vue d'ensemble des fonctionnalités chiffrée de configuration

Cette section décrit le processus qui se produit quand des fichiers chiffrés de téléphone de configuration sont utilisés dans le CUCM.

Quand vous activez cette caractéristique, remettez à l'état initial le téléphone, et téléchargez le fichier de configuration, vous recevez une demande du fichier avec une **extension .cnf.xml.sgn :**

Cependant, après que la caractéristique de configuration chiffrée soit activée sur le CUCM, le service TFTP ne génère plus un fichier de configuration complète avec l'**extension .cnf.xml.sgn.** Au lieu de cela, il génère le fichier de configuration partiel, suivant les indications de l'exemple

suivant.

> **Note**: Quand vous utilisez cette méthode pour la première fois, le téléphone compare les informations parasites de MD5 du certificat de téléphone dans le fichier de configuration aux informations parasites de MD5 localement - du certificat significatif (LSC) ou des Certificats installés par fabrication (MIC).

```
HTTP/1.1 200 OK
Content-length: 759
Cache-Control: no-store
Content-type: */*
<fullConfig>False</fullConfig>
<loadInformation>SIP75.9-3-1SR2-1S</loadInformation>
<ipAddressMode>0</ipAddressMode>
<capfAuthMode>0</capfAuthMode>
<capfList>
<capf>
<phonePort>3804</phonePort>
<processNodeName>10.48.46.4</processNodeName>
</capf>
</capfList>
<certHash></certHash>
<encrConfig>true</encrConfig>
</device>
```

Si le téléphone identifie un problème, il tente d'initier une session avec le CAPF, à moins que l'authentication mode CAPF s'assortisse *par des chaînes d'authentification*, dans ce cas vous devez manuellement écrire la chaîne. Voici quelques problèmes que le téléphone pourrait identifier :

- Les informations parasites ne s'assortissent pas.
- Le téléphone ne contient pas un certificat.
- La valeur de MD5 est vide (comme dans l'exemple précédent).

> **Note**: Le téléphone initie une session de Transport Layer Security (TLS) au service CAPF sur le port 3804 par défaut.

Le certificat CAPF doit être connu pour le téléphone, ainsi il doit être inclus dans le fichier ITL ou le fichier de la liste de confiance de certificat (CTL) (si les cluster run dans le mode mixte).

Après que la transmission CAPF soit établie, le téléphone envoie les informations au CAPF au sujet du LSC ou de la MIC qui est utilisée. Le CAPF alors extrait la clé publique de téléphone du LSC ou de la MIC, génère des informations parasites de MD5, et enregistre les valeurs pour les informations parasites de clé publique et de certificat dans la base de données CUCM.

```
admin:run sql select md5hash,name from device where name='SEPA45630BBFA40'
md5hash name
================================ ===============
6e566143c1c14566c9da943d949a79c8 SEPA45630BBFA40
```

Après que la clé publique soit enregistrée dans la base de données, le téléphone remet à l'état initial et demande un nouveau fichier de configuration. Les tentatives de téléphone de télécharger le fichier de configuration avec l'**extension cnf.xml.sgn de nouveau**.

```
HTTP/1.1 200 OK
Content-length: 759
Cache-Control: no-store
Content-type: */*
<fullConfig>False</fullConfig>
<loadInformation>SIP75.9-3-1SR2-1S</loadInformation>
<ipAddressMode>0</ipAddressMode>
<capfAuthMode>0</capfAuthMode>
<capfList>
<capf>
<phonePort>3804</phonePort>
<processNodeName>10.48.46.4</processNodeName>
</capf>
</capfList>
<certHash>6e566143c1c14566c9da943d949a79c8</certHash>
<encrConfig>true</encrConfig>
</device>
```

Le téléphone compare le **cerHash** de nouveau, et s'il ne détecte pas le problème, il télécharge le fichier de configuration chiffré avec l'**extension .cnf.xml.enc.sgn.**

```
............c..)CN=cucm85;OU=It;O=Cisco;L=KRK;ST=PL;C=PL....Z.........)CN=cucm85;
OU=It;O=Cisco;L=KRK;ST=PL;C=PL...........
..........C.<...Y6.Lh.|(..w+..,.0.a.&.
O..........V....T...Z..R^..f....|.=.e.@...5...........G...[.........n.........=
.A..H.(....Z...{.!%[.. SEPA45630BBFA40.cnf.xml.enc.sgn....R.DD..M............
Uu.C..@...........
...................m.b.......6y ..x.^b..-8.^..^'.4.<Wb.n.....5...we.0@..g..
V7.,..r.9
Qs>..).w....pt/...}A.']
.r.t%G..d_.;u.rEI.pr.F
.....M..r...o.N
.=..g.^P....Pz....J..E.S...d|Z).....J..&..I....7.r..g8.{f..o.....:.~..U...5G+V.
[...]
```

Caractéristique de configuration chiffrée par enable

Afin d'activer les fichiers chiffrés de téléphone de configuration, vous devez créer un nouveau (ou éditer un courant) profil de degré de sécurité de téléphone et l'assigner au téléphone. Terminez-vous ces étapes afin d'activer la caractéristique de configuration chiffrée sur le CUCM :

1. Connectez-vous dans la page de gestion CUCM et naviguez vers le **profil de système > de Sécurité > de degré de sécurité de téléphone** :

2. Copiez un courant, ou créez un nouveau, téléphonez le profil de Sécurité et cochez la case de **config chiffrée par TFTP** :

3. Assignez le profil au téléphone :

Dépannez

Terminez-vous ces étapes afin de dépanner des questions de système en vue de la caractéristique de configuration chiffrée :

1. Assurez-vous que le service CAPF est en activité et fonctionne correctement sur le noeud de Publisher dans la batterie CUCM.

2. Téléchargez le fichier de configuration partiel et le vérifiez que le port et l'adresse IP du service CAPF sont accessibles du téléphone.

3. Vérifiez la transmission de TCP sur le port 3804 au noeud de Publisher.

4. Exécutez la commande précédemment mentionnée du SQL (SQL) afin de vérifier si le service CAPF a des informations sur le LSC ou la MIC qui est utilisée par le téléphone.

5. Si la question persiste toujours, vous pourriez être requis de collecter les informations complémentaires du système. Redémarrez le téléphone et collectez ces informations :

   Messages de console de téléphoneLogs de Cisco TFTPLogs de Cisco CAPFCaptures de paquet du CUCM et du téléphone

Référez-vous à ces ressources pour des informations supplémentaires sur la façon exécuter des captures de paquet du CUCM et du téléphone :

- Collecter des suivis CUCM de CUCM 8.6.2 pour un SR TAC
- Capture des parquets sur le modèle appliance Unified Communications Manager
- Collecter une capture de paquet d'un téléphone IP de Cisco

Dans les logs et les captures de paquet, vous devez s'assurer que le processus décrit dans les sections précédentes fonctionne correctement. Spécifiquement, vérifiez cela :

- Le téléphone télécharge le fichier de configuration partiel avec les informations correctes CAPF.
- Le téléphone se connecte par l'intermédiaire du TLS au service CAPF, et cela les informations sur le LSC ou la MIC est mis à jour dans la base de données.
- Le téléphone télécharge le plein fichier de configuration chiffré.