Régénération de certificat CUCM/processus de renouvellement

Contenu

Introduction

Ce document fournit une procédure recommandée et pas à pas pour régénérer des Certificats utilisés dans la version 8.x et ultérieures de Cisco Unified Communications Manager (CUCM). La Sécurité par la caractéristique par défaut (ITL) et le mode mixte (CTL) sont également soient couverts afin d'éviter toutes les pannes peu désirées. Par exemple, comment éviter les questions ou les téléphones d'enregistrement de téléphone qui ne reçoivent pas des modifications ou des micrologiciels de configuration.

> **Attention** : Il est toujours recommandé pour se terminer la régénération de certificat dans une fenêtre de maintenance.

Aperçu

Ce document discute le procédé de régénération de certificat pour ces services :

- CallManager

- CAPF (fonction de proxy d'autorité de certification)
- IPsec
- Tomcat
- TV (service de vérification de confiance)
- ITLRecovery (seulement pour CUCM 10.X et plus tard)
- téléphone-VPN-confiance
- téléphone-SAST-confiance
- téléphone-confiance
- téléphone-ctl-confiance

Aussi bien que ces Certificats de téléphone :

- LSC (localement - Certificats significatifs)
- MICs (Certificats installés par fabricant)

Composants utilisés

Toutes les sorties et captures d'écran affichées dans ce document sont basées sur la version 9.1(2)SU2a CUCM, toutefois la procédure présentée peut être utilisée avec la version 8.x et ultérieures CUCM. Des différences qui sont particularité de release sont mentionnées dans les sections appropriées.

Les informations dans ce document ont été basées sur des périphériques dans un environnement de travaux pratiques qui a commencé par une configuration (par défaut) effacée. Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelles commande et mesure prises.

Quand régénérer des Certificats

La plupart des Certificats utilisés dans CUCM après qu'une installation fraîche soient les Certificats auto-signés délivrés, par défaut, pendant cinq années. Notez que la plage de temps de cinq ans actuellement ne peut pas être modifiée pour être un intervalle plus court de temps sur CUCM. Cependant, un Autorité de certification (CA) peut délivrer des Certificats pour presque n'importe quelle plage de temps.

Il y a également quelques Certificats de confiance (tels que la CAPF-confiance et la CallManager-confiance) qui sont préchargés et ont une plus longue période de validité. Par exemple, « Cisco fabriquant le CA » délivrent un certificat est fourni sur des mémoires de confiance CUCM aux caractéristiques spécifiques et n'expirera pas avant l'année 2029.

Des Certificats devraient être régénérés avant qu'ils expirent. Quand les Certificats sont sur le point d'expirer vous recevrez des avertissements dans RTMT (visualiseur de Syslog) et un email avec la notification sera envoyé si configuré.

Un exemple d'une notification d'expiration de certificat qui détaille le certificat de "CUCM01.der" expirera « Lun le 19 mai 14:46" sur le serveur que CUCM02 sur la mémoire « Tomcat-confiance " de confiance est affiché ici :

```
At Fri Sep 05 02:00:56 CEST 2014 on node 192.168.1.2, the following
SyslogSeverityMatchFound events generated:
```

```
SeverityMatch : Critical

MatchedEvent : Sep 5 02:00:06 CUCM02 local7 2 : 864: CUCM02.localdomain:
Sep 05 2014 00:00:06.433 UTC : %UC_CERT-2-CertValidfor7days:
%[Message=Certificate expiration Notification. Certificate name:CUCM01.der
Unit:tomcat-trust Type:own-cert Expiration:Mon May 19 14:46:]
[AppID=Cisco Certificate Monitor][ClusterID=][NodeID=CUCM02]:
Alarm to indicate that Certificate has Expired or Expires in less than seven days

AppID : Cisco Syslog Agent

ClusterID :

NodeID : CUCM02

TimeStamp : Fri Sep 05 02:00:16 CEST 2014
```

Si les Certificats de service (les mémoires de certificat avec lesquelles ne sont pas étiquetés « - confiance ») sont déjà expirés il est encore possible de les régénérer. Maintenez dans l'esprit que les Certificats expirés pourraient avoir une incidence sur votre fonctionnalité CUCM, dépendant sur la configuration de la batterie. Des considérations sont discutées dans les sections suivantes.

Entretenez l'incidence par la mémoire de certificat

Il est essentiel pour la bonne fonctionnalité du système pour avoir tous les Certificats mis à jour à travers la batterie CUCM. Si vos Certificats sont expirés ou non valide ils pourraient de manière significative affecter la fonctionnalité normale du système. Une liste d'éventuels problèmes que vous pourriez avoir quand les Certificats spécifiques l'uns des sont non valides ou expiré est affiché ici. L'incidence pourrait différer personne à charge sur votre installation de système.

CallManager.pem

- Téléphones chiffrés/authentifiés ne s'enregistrent pas.
- TFTP non fait confiance (les téléphones ne reçoivent pas les fichiers de configuration signés et/ou les fichiers ITL).
- Les services de téléphonie pourraient être affectés.
- Les joncteurs réseau de Protocole SIP (Session Initiation Protocol) ou les ressources sécurisés en medias (passerelles de conférence, Media Termination Point (MTP), Xcoders, et ainsi de suite) ne s'enregistreront pas ou fonctionneront.
- La demande AXL échoue.

Tomcat.pem

- Les téléphones ne peuvent pas accéder à des services de HTTPs hébergés sur le noeud CUCM, tel que le répertoire d'entreprise.
- Questions GUI du Web de CUCM, telles qu'incapable aux pages de service d'accès d'autres Noeuds dans la batterie.
- La batterie de croix de mobilité d'extension ou de mobilité d'extension émet.

CAPF.pem

- Les téléphones n'authentifient pas pour le téléphone VPN, le 802.1x, ou le proxy de téléphone.
- Ne peut pas délivrer des Certificats LSC pour les téléphones.
- Les fichiers de configuration chiffrés ne fonctionnent pas.

IPSec.pem

- Le cadre de reprise du système de Reprise sur sinistre (jeu rouleau-tambour) /Disaster (DRF) ne pourrait pas fonctionner correctement.
- Les tunnels d'IPsec à la passerelle (gw) à d'autres batteries CUCM ne fonctionnent pas.

TV (service de vérification de confiance)

- Le téléphone ne peut pas authentifier le service HTTPS. Le téléphone ne peut pas authentifier des fichiers de configuration (ceci peut affecter presque tout sur CUCM).

téléphone-VPN-confiance

- Le téléphone VPN ne fonctionnera pas, parce que l'URL HTTPS du VPN ne peut pas être authentifié.

  Remarque: Si ceci n'existe pas ne vous inquiétez pas. C'est seulement pour des configurations spécifiques.

téléphone-SAST-confiance

- CTL/eTokens précédent ne pourra pas mettre à jour ou modifier CTL.

  Remarque: Si ceci n'existe pas ne vous inquiétez pas. C'est seulement pour des configurations spécifiques.

téléphone-confiance et téléphone-ctl-confiance

- La Messagerie vocale visuelle avec l'Unity ou l'Unity Connection ne fonctionnera pas.

  Remarque: Si ceci n'existe pas ne vous inquiétez pas. C'est seulement pour des configurations spécifiques.

LSC et MICs

- Les téléphones ne s'enregistrent pas, téléphone n'authentifie pas pour téléphoner le VPN, le proxy de téléphone, ou le 802.1x.

  Remarque: MICs sont sur la plupart des modèles de téléphone par défaut. Des LSC sont signés par CAPF et cinq dernières années par défaut. Des clients logiciels tels que le CIPC (Cisco IP Communicator) et le Jabber ne font pas installer une MIC.

Créez une sauvegarde jeu rouleau-tambour

Il est recommandé pour créer une sauvegarde jeu rouleau-tambour avant que vous exécutiez tous les changements majeurs comme ceci. Les sauvegardes CUCM DRF sauvegarderont tous les Certificats dans la batterie. Tout le jeu rouleau-tambour de sauvegarde/procédures de restauration peut être trouvé à Cisco « guide d'administration système de Reprise sur sinistre pour Cisco Unified Communications Manager ».

Attention : Maintenez dans l'ID de bogue Cisco CSCtn50405 d'esprit, sauvegarde CUCM DRF fait pas les Certificats de sauvegarde.

Déterminez si la batterie est dans le mode mixte

Afin de déterminer si vous exécutez une batterie CTL/Secure/Mixed-Mode, choisissez la **gestion de Cisco Unified CM > le System > Enterprise Parameters > la security mode de batterie (0 == Non-sécurisés ; 1 mode mixte de ==)**.

Si la batterie est dans le mode mixte

Si vous exécutez une batterie CUCM dans le mode mixte, ceci signifie que le fichier CTL doit être après tout les modifications à jour de certificat. La procédure sur la façon dont faire ceci est dans la documentation de guide de la Sécurité de Cisco. Cependant, soyez sûr que vous faites eToken au moins on de l'initiation d'origine de la caractéristique de mode mixte et le mot de passe d'eToken est connu.

> Remarque: Une mise à jour du CTL ne se produit pas automatiquement (comme elle fait en cas de fichier ITL). Il doit être terminé manuellement par l'administrateur avec le client CTL ou la commande CLI.

Dans CUCM 10.X et plus tard vous pouvez mettre la batterie dans le mode mixte de deux manières :

- Commande CLI - si cette méthode est utilisée alors votre fichier CTL est signée avec le certificat CallManager.pem du serveur de Publisher. `admin:`**`show ctl`**
```
The checksum value of the CTL file:
0c05655de63fe2a042cf252d96c6d609(MD5)
8c92d1a569f7263cf4485812366e66e3b503a2f5(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Fri Mar 06 19:45:13 CET 2015

[...]

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1156
2 DNSNAME 16 cucm-1051-a-pub
3 SUBJECTNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
6 SERIALNUMBER 16 70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 694 E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21
A5 A3 8C 9C (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```
- Client CTL - si cette méthode est utilisée alors votre fichier CTL est signée avec un des eTokens de matériel. `admin:`**`show ctl`**
```
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)
```

```
Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Remarque: Vous pouvez se déplacer entre la méthode utilisée avec le mode mixte CUCM avec Tokenless CTL.

La personne à charge sur la méthode utilisée pour sécuriser votre batterie, une procédure appropriée de mise à jour CTL doit être utilisée. Réexécutez le client CTL ou sélectionnez la commande de **CTLfile de mise à jour de ctl d'utils du** CLI.

Vérifiez la Sécurité par défaut sur la batterie

La manière d'éviter des questions ITL est importante, parce que les questions ITL peuvent faire échouer beaucoup de caractéristiques ou le téléphone refusera de se conformer à toutes les modifications aux configurations. Des questions ITL peuvent être évitées de ces deux manières.

Utilisez « préparent la batterie pour le repositionnement à la caractéristique pré de 8.0"

Cette caractéristique « masque » votre ITL sur tous les serveurs, ainsi les téléphones feront confiance à n'importe quel serveur TFTP. Les services de téléphonie (par exemple, mobilité d'extension) ne travailleront pas quand ce paramètre est placé pour rectifier. Cependant, les utilisateurs pourront continuer à faire et recevoir des appels téléphoniques de base.

Remarque: Une modification à ce paramètre fait REMETTRE À L'ÉTAT INITIAL TOUS LES TÉLÉPHONES.

Une fois que cette caractéristique est placée, tous les serveurs TFTP doivent être redémarrés (afin de fournir la nouvelle ITL) et tout le besoin de téléphones d'être remis à l'état initial afin de les forcer pour demander la nouvelle ITL de « blanc ». Une fois les modifications de certificat sont terminées et tous les services nécessaires ont été redémarrés, cette caractéristique peuvent être placés de nouveau à « faux », au service TFTP redémarré, et à la remise de téléphone (ainsi au téléphone peut obtenir le fichier valide ITL). Alors toutes les caractéristiques continueront à fonctionner comme le faisaient précédemment elles.

Certificats régénérés dans la commande spécifique

Cette procédure fournit à un serveur TFTP fichier valide/mis à jour ITL d'un serveur de confiance TFTP qui est disponible.

1. Service TFTP d'arrêt sur le serveur primaire TFTP.
2. Apportez des modifications sur les Certificats de serveur primaires TFTP (comme nécessaire).
3. Remettez à l'état initial les téléphones (afin d'obtenir un nouveau fichier ITL du serveur secondaire TFTP) - la personne à charge sur laquelle des Certificats sont régénérés, ceci pourrait se produire automatiquement.
4. Une fois que les téléphones sont retournés, mettez sur pied le service TFTP du serveur primaire TFTP.
5. Apportez les modifications de certificat sur le serveur secondaire TFTP.
6. Remettez à l'état initial les téléphones (afin d'obtenir un nouveau fichier ITL du serveur primaire TFTP).

   Attention : N'éditez pas les Certificats sur les deux serveurs TFTP en même temps. Ceci ne donne aux téléphones aucun serveur TFTP pour faire confiance et exige de l'administrateur local de retirer manuellement l'ITL de tous les téléphones.

Retirez et régénérez les Certificats dans CUCM

Seulement des Certificats de service (les mémoires de certificat avec lesquelles ne sont pas étiquetés « - confiance ») peuvent être régénérés. Des Certificats dans les mémoires de confiance (les mémoires de certificat avec lesquelles sont étiquetés « - confiance ») doivent être supprimés, car ils ne peuvent pas être régénérés.

> **Attention** : Rendez-vous compte de l'ID de bogue Cisco CSCut58407 - Les périphériques ne devraient pas redémarrer quand CAPF/CallManager/TV-confiance est enlevé.

Délivrez un certificat après tout les modifications, le service respectif doit être redémarré pour prendre la modification. Ceci est couvert dans après régénération/suppression de section de Certificats.

> **Attention** : Rendez-vous compte de l'ID de bogue Cisco CSCto86463 - Les Certificats supprimés réapparaissent, incapable de retirer des Certificats de CUCM. C'est une question où les Certificats supprimés continuent à réapparaître après suppression. Suivez le contournement dans le défaut.

Certificats régénérés par l'intermédiaire du CLI

> **Attention** : Les régénérations des Certificats déclenche une mise à jour automatique des fichiers ITL dans la batterie, qui déclenche une remise batterie batterie de téléphone logiciel pour permettre à des téléphones pour déclencher une mise à jour de leur ITL de gens du

pays. Ceci est concentré sur des régénérations de certificat CAPF et de CallManager, mais peut se produire avec d'autres mémoires de certificat dans CUCM, tel que Tomcat.

CAPF régénéré

Lors de la régénération, le certificat CAPF se télécharge automatiquement CAPF-confiance et CallManager-confiance. En outre, CAPF a toujours une seule en-tête de nom du sujet, ainsi des Certificats précédemment utilisés CAPF seront retenus et utilisés pour l'authentification.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

> Remarque: Si un certificat CAPF obtient expiré, les téléphones qui utilisent le LSC ne pourront pas s'enregistrer à CUCM parce que CUCM rejette leur certificat. Cependant, vous pouvez encore générer un nouveau LSC pour le téléphone avec le nouveau certificat CAPF. Quand vous redémarrez le téléphone qu'il télécharge la configuration et entre en contact avec alors CAPF afin de mettre à jour le LSC. Après que le LSC soit mis à jour, le téléphone s'enregistre comme il faudrait. Ceci fonctionne tant que un nouveau certificat CAPF est dans le fichier ITL et le téléphone téléchargés et a fait confiance au certificat qui l'a signé (callmanager.pem).

CallManager régénéré

Lors de la régénération, le CallManager se télécharge automatiquement CallManager-confiance.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
```

```
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

IPsec régénéré

Lors de la régénération, le certificat d'IPsec se télécharge automatiquement ipsec-confiance.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Tomcat régénéré

Lors de la régénération, le certificat de Tomcat se télécharge automatiquement Tomcat-confiance.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
```

```
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

TV régénérées

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Ce qui à prévoir

Quand vous régénérez des Certificats par l'intermédiaire du CLI, vous êtes prié de vérifier cette modification. Tapez **oui** et appuyez sur **entrent**.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Retirez les Certificats par l'intermédiaire du CLI

Retirez les Certificats de CAPF-confiance

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Retirez les Certificats de CallManager-confiance

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Retirez les Certificats d'ipsec-confiance

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)
```

```
Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Retirez les Certificats de Tomcat-confiance

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Retirez les Certificats de TV-confiance

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
```

```
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Certificats régénérés par l'intermédiaire du GUI de Web

CAPF régénéré

Lors de la régénération, le certificat CAPF se télécharge automatiquement CAPF-confiance et CallManager-confiance. En outre, le certificat CAPF a toujours une seule en-tête de nom du sujet, ainsi des Certificats précédemment utilisés CAPF sont retenus et utilisés pour l'authentification.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

CallManager régénéré

Lors de la régénération, le certificat CAPF se télécharge automatiquement CallManager-confiance.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
```

```
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

IPsec régénéré

Lors de la régénération, le certificat d'IPsec se télécharge automatiquement ipsec-confiance.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Tomcat régénéré

Lors de la régénération, le certificat de Tomcat se télécharge automatiquement Tomcat-confiance.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
```

```
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

TV régénérées

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Retirez les Certificats par l'intermédiaire du GUI de Web

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Après régénération/suppression des Certificats

Après que vous retiriez ou régénériez un certificat d'une mémoire de certificat, le service respectif doit être redémarré afin de prendre la modification.

Enregistrez	Entretenez pour redémarrer	Comment (== CLI de C ; GUI de Web de == W)
Tomcat	Tomcat	C : reprise Cisco Tomcat de service d'utils G : Utilité > Tools > Control Center de Cisco Unified - L caractéristique entretient > (serveur choisi) > « Cisco CallManager » choisi > reprise
CallManager	CallManager ; TFTP	ET G : Utilité > Tools > Control Center de Cisco Unified - L caractéristique entretient > (serveur choisi) > « tftp de C choisi > reprise
CAPF	CAPF (sur Publisher seulement)	G : Utilité > Tools > Control Center de Cisco Unified - L caractéristique entretient > (serveur choisi) > « fonction proxy d'autorité de certification de Cisco » choisie > repr
TV	Service de vérification de confiance (sur le serveur respectif)	G : Utilité > Tools > Control Center de Cisco Unified - Le services > (serveur choisi) > « Cisco choisi font confianc service de vérification » > reprise
ipsec	Gens du pays de Cisco DRF (sur tous les Noeuds) ; Maître de Cisco DRF (sur Publisher)	C : gens du pays de Cisco DRF de reprise de service d' ET C : maître de Cisco DRF de reprise de service d'utils

Installez/mise à jour LSC au téléphone

Si le certificat CAPF a été régénéré, alors des Certificats LSC pour tous les téléphones dans la nécessité de batterie d'être mis à jour avec le LSC signé par le nouveau certificat CAPF.

1. Choisissez l'**utilité > l'activation de service CUCM**. Lancez la fonction de proxy de fournisseur de Cisco CTL et d'autorité de certification de Cisco sur le serveur d'éditeur.
2. De CUCM CCMAdmin, choisissez le **Device > Phone.** Sélectionnez le téléphone IP que vous voulez provision un LSC en fonction.
3. Dans la page de configuration de périphérique sous l'exécution de certificat, choisissez **installent/mises à jour > par la chaîne null**.
4. Sauvegardez la configuration de téléphone dans CCMAdmin et choisissez **appliquent le config**.

Si le téléphone a des ennuis avec l'installation du LSC, terminez-vous ces actions au téléphone :

Quand les remises de téléphone, vont au téléphone et au sélectionnez Settings physiques **> (6) configuration de sécurité > (4) LSC > ** #** (cette exécution déverrouille le GUI et nous permet pour continuer à l'étape suivante) **> mise à jour** (la mise à jour ne sera pas visible jusqu'à ce que vous exécutiez l'étape précédente) **> soumettent**.

N'assignez aucun Certificats à un téléphone à moins que ce soit un téléphone Sans fil (7921/25). Les téléphones Sans fil utilisent les autorités de certification de tiers (CA) afin de s'authentifier.

Conclusion

Au cas où vous vous exécuteriez dans une question ou avez besoin de l'assistance avec cette procédure, entrez en contact avec le centre d'assistance technique Cisco (TAC) pour l'assistance. Dans ce cas, maintenez votre sauvegarde DRF disponible car elle sera utilisée en dernier recours afin de restaurer le service si le TAC ne peut pas faire ainsi par d'autres méthodes.