Processus de régénération/renouvellement du certificat CUCM

Contenu

Introduction

Ce document fournit une procédure étape par étape recommandée pour régénérer les certificats utilisés dans Cisco Unified Communications Manager (CUCM) version 8.x et ultérieures. La fonction de sécurité par défaut (ITL) et le mode mixte (CTL) sont également abordés afin d'éviter toute situation non désirée, notamment les problèmes d'enregistrement de téléphones ou des changements de configuration ou de micrologiciel refusés.

> **Attention** : Il est toujours recommandé de terminer la régénération du certificat durant une période de maintenance.

Aperçu

Le présent document traite du processus de régénération des certificats pour les services suivants :

- CallManager
- CAPF (Certificate Authority Proxy Function)

- IPsec
- Tomcat
- TVS (Trust Verification Service)
- ITLRecovery (seulement pour CUCM 10.X et versions ultérieures)
- phone-vpn-trust
- phone-sast-trust
- phone-trust
- phone-ctl-trust

Ainsi que les certificats téléphoniques suivants :

- LSC (Locally Significant Certificates)
- MIC (Manufacturer Installed Certificates)

Composants utilisés

Toutes les sorties et captures d'écran présentées dans ce document sont basées sur CUCM version 9.1(2)SU2a; la procédure présentée peut aussi être utilisée avec CUCM version 8.x et ultérieures. Les différences propres à chaque version sont mentionnées dans les sections appropriées.

Les informations contenues dans ce document sont basées sur des appareils dans un environnement de laboratoire qui ont commencé avec une configuration par défaut (vierge). Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible de vos commandes et de vos actions.

Quand régénérer les certificats?

La plupart des certificats utilisés dans CUCM après une nouvelle installation sont des certificats autosignés émis, par défaut, pour cinq ans. Il est à noter que la période de cinq ans ne peut actuellement pas être modifiée pour être plus courte avec CUCM. Toutefois, une autorité de certification (AC) peut délivrer des certificats pour presque n'importe quel intervalle de temps.

Il existe également des certificats de confiance (tels que CAPF-trust et CallManager-trust) qui sont préchargés et ont une période de validité plus longue. Par exemple, le certificat « Cisco Manufacturing CA » est fourni par les magasins CUCM-trust avec des caractéristiques spécifiques et n'expirera pas avant l'année 2029.

Les certificats devraient être régénérés avant leur expiration. Lorsque les certificats sont sur le point d'expirer, vous recevrez des avertissements dans RTMT (Syslog Viewer) et un courriel à cet effet, si le système est configuré pour en créer un.

Voici un exemple d'un avis d'expiration de certificat qui détaille le certificat « CUCM01.der » venant à échéance le « Lun Mai 19 14:46 » sur le serveur CUCM02 sur le magasin tomcat-trust :

```
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 (provenant de magasins qui ne sont pas étiquetés avec « -trust ») sont expirés, il est possible de les régénérer. Gardez à l'esprit que les certificats expirés peuvent avoir un impact sur votre fonctionnalité CUCM, selon la configuration de la grappe. Les aspects à considérer sont abordés dans les sections suivantes.

Impact du service par le magasin de certificats

Il est essentiel pour la bonne fonctionnalité du système d'avoir tous les certificats mis à jour à travers la grappe CUCM. Si vos certificats sont expirés ou invalides, ils peuvent entraver de manière significative le fonctionnement normal du système. Une liste des problèmes potentiels que vous pourriez avoir lorsqu'un certificat en particulier est invalide ou expiré est affichée ici. L'impact peut varier en fonction de la configuration de votre système.

CallManager.pem

- Les téléphones cryptés/authentifiés ne s'enregistrent pas.
- TFTP n'est pas fiable (les téléphones n'acceptent pas les fichiers de configuration signés ou les fichiers ITL).
- Les services téléphoniques pourraient être touchés.
- Les liaisons SIP (Session Initiation Protocol) sécurisées ou les ressources média (ponts pour appels de conférence, points de terminaison média (MTP), codeurs X, etc.) ne sont pas enregistrés 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.
- Problèmes liés à l'interface graphique Web du CUCM, comme l'impossibilité d'accéder aux pages de service à partir d'autres nœuds de la grappe.
- Problèmes avec Extension Mobility ou Extension Mobility Cross Cluster.

CAPF.pem

- Les téléphones ne s'authentifient pas pour les services « Phone VPN », « 802.1x » ou « Phone Proxy ».
- Échec de livraison de certificats LSC pour les téléphones.
- Les fichiers de configuration cryptés ne fonctionnent pas.

IPSec.pem

- Le système ou cadre de reprise après sinistre (DRS ou DRF) ne fonctionne pas correctement.

- Les tunnels IPsec vers d'autres grappes CUCM ne fonctionnent pas.

TVS (Trust Verification Service)

- Le téléphone ne peut pas authentifier le service HTTPS. Le téléphone ne peut pas authentifier les fichiers de configuration (cela peut toucher presque tout sur CUCM).

phone-vpn-trust

- Le VPN du téléphone ne fonctionnera pas, car l'adresse URL HTTPS du VPN ne peut pas être authentifiée.

  Note: Si cela n'existe pas, ne vous inquiétez pas; ceci n'est valable que pour des configurations particulières.

phone-sast-trust

- Les CTL/eTokens précédents ne peuvent pas mettre à jour ou modifier les CTL.

  Note: Si cela n'existe pas, ne vous inquiétez pas; ceci n'est valable que pour des configurations particulières.

phone-trust and phone-ctl-trust

- La messagerie vocale visuelle avec Unity ou la connexion Unity ne fonctionne pas.

  Note: Si cela n'existe pas, ne vous inquiétez pas; ceci n'est valable que pour des configurations particulières.

LSC et MIC

- Les téléphones ne s'enregistrent pas ou ne s'authentifient pas au VPN téléphonique, au proxy téléphonique ou au 802.1x.

  Note: Par défaut, les MIC sont sur la plupart des modèles de téléphone. Les LSC sont signés par le CAPF et durent cinq ans par défaut. Les logiciels clients tels que CIPC (Cisco IP Communicator) et Jabber n'ont pas de MIC installé.

Créer une sauvegarde DRS

Il est recommandé de créer une sauvegarde DRS avant d'effectuer des modifications majeures comme celle-ci. Les sauvegardes CUCM DRF sauvegarderont tous les certificats de la grappe. Toutes les procédures de sauvegarde ou de restauration du DRS se trouvent dans le « Disaster Recovery System Administration Guide for Cisco Unified Communications Manager ».

> **Attention** : Gardez à l' esprit que l' ID d' bogue Cisco CSCtn50405 , CUCM Sauvegarde DRF pas sauvegarder les certificats .

Déterminer si la grappe est en mode mixte

Pour déterminer si vous utilisez une grappe CTL/sécurisée/mode mixte, choisissez **Cisco Unified**

CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 === Non-Secure ; 1 == Mixed Mode).

Si la grappe est en mode mixte

Si vous exécutez une grappe CUCM en mode mixte, cela signifie que le fichier CTL doit être mis à jour après tous les changements de certificat. La procédure à suivre se trouve dans le Guide de sécurité de Cisco. Cependant, assurez-vous d'avoir au moins un eToken de l'initialisation originale du mode mixte et de connaître le mot de passe pour eToken.

> **Note**: Une mise à jour de la CTL ne se fait pas automatiquement (contrairement au fichier ITL). Il doit être complété manuellement par l'administrateur avec la commande CTL Client ou par l'interface de ligne de commande.

Dans CUCM 10.X et les versions ultérieures, vous pouvez mettre la grappe en mode mixte de deux façons :

- Interface de ligne de commande – si cette méthode est utilisée, votre fichier CTL est signé avec le certificat CallManager.pem du serveur 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, votre fichier CTL est signé avec l'un des eTokens matériels.

```
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.
```

Note: Vous pouvez passer d'une méthode à l'autre avec « CUCM Mixed Mode with Tokenless CTL ».

Selon la méthode utilisée pour sécuriser votre grappe, une procédure de mise à jour CTL appropriée doit être utilisée. Relancez le client CTL ou entrez la commande **utils ctl update CTLfile** depuis la ligne de commande.

Vérifier la sécurité par défaut de la grappe

Il est important d'éviter les problèmes d'ITL, car ils peuvent entraîner la défaillance de nombreuses fonctionnalités ou causer le téléphone à refuser tout changement de configuration. Les problèmes d'ITL peuvent être évités de ces deux manières.

Utiliser la fonction « Préparer la grappe pour le retour à la version 8.0 »

Cette fonction « efface » votre ITL sur tous les serveurs, de sorte que les téléphones feront confiance à n'importe quel serveur TFTP. Les services téléphoniques (par exemple, la mobilité de poste) ne fonctionneront PAS lorsque ce paramètre est défini comme « Vrai ». Toutefois, les utilisateurs pourront continuer à faire et à recevoir des appels téléphoniques de base.

Note: Une modification de ce paramètre provoque la réinitialisation de tous les téléphones.

Une fois cette fonction activée, tous les serveurs TFTP doivent être redémarrés (afin de fournir la nouvelle ITL) et tous les téléphones doivent être réinitialisés afin de les forcer à demander la nouvelle ITL « vierge ». Une fois que les changements de certificat sont terminés et que tous les services nécessaires ont été redémarrés, cette fonction peut être remise à « Faux », le service TFTP peut être redémarré et les téléphones peuvent être réinitialisés (afin d'obtenir le fichier ITL valide). Ensuite, toutes les fonctions continueront à fonctionner comme avant.

Régénérer les certificats dans un ordre particulier

Cette procédure fournit au serveur TFTP un fichier ITL valide/mis à jour provenant d'un serveur TFTP de confiance et disponible.

1. Arrêtez le service TFTP sur le serveur TFTP primaire.

2. Effectuez des modifications sur les certificats du serveur TFTP primaire (si nécessaire).
3. Réinitialisez les téléphones (afin d'obtenir un nouveau fichier ITL à partir du serveur TFTP secondaire) – en fonction des certificats qui sont régénérés, cela peut se produire automatiquement.
4. Une fois que les téléphones ont été réinitialisés, démarrez le service TFTP du serveur TFTP primaire.
5. Modifiez les certificats sur le serveur TFTP secondaire.
6. Réinitialisez les téléphones (afin d'obtenir un nouveau fichier ITL à partir du serveur TFTP primaire).

> **Attention** : NE MODIFIEZ PAS les certificats sur les deux serveurs TFTP en même temps. Il n'y aurait alors aucun serveur TFTP de confiance et exigerait de l'administrateur local qu'il retire manuellement l'ITL de tous les téléphones.

Supprimer et régénérer des certificats dans CUCM

Seuls les certificats de service (provenant de magasins qui ne portent pas l'étiquette « -trust ») peuvent être régénérés. Les certificats provenant de magasins portant l'étiquette « -trust » doivent être supprimés, car ils ne peuvent pas être régénérés.

> **Attention** : Attention au bogue CSCut58407 - Les périphériques ne devraient pas redémarrer lorsque CAPF / CallManager / TVS-trust est supprimé.

Une fois un certificat modifié, le service visé doit être redémarré pour recevoir les modifications. La section « Après la régénération/suppression de certificats » aborde ce sujet plus en détail.

> **Attention** : Attention au bogue CSCto8646463 - Les certificats supprimés réapparaissent; incapable de supprimer des certificats de CUCM. Il s'agit d'un problème où les certificats supprimés continuent de réapparaître après la suppression. Suivez la solution de contournement dans la fiche du bogue.

Régénérer les certificats avec l'interface de ligne de commande

> **Attention** : Les régénérations de certificats déclenchent une mise à jour automatique des fichiers ITL au sein de la grappe, ce qui déclenche une réinitialisation du téléphone logiciel à l'échelle de la grappe pour permettre aux téléphones de déclencher une mise à jour de leur ITL local. Les régénérations de certificats CAPF et CallManager sont couramment à l'origine d'une telle situation, mais cela peut se produire avec d'autres listes de certificats dans CUCM, comme Tomcat.

Régénération du CAPF

Lors de la régénération, le certificat CAPF se télécharge automatiquement dans CAPF-trust et CallManager-trust. De plus, le CAPF a toujours un nom unique, de sorte que les certificats du CAPF utilisés précédemment seront conservés 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.
```

> **Note**: Si un certificat du CAPF arrive à expiration, les téléphones qui utilisent le LSC ne pourront pas s'enregistrer avec le CUCM parce que le CUCM refusera leur certificat. Toutefois, vous pouvez toujours générer un nouveau LSC pour un téléphone avec le nouveau certificat CAPF. Lorsque vous redémarrerez le téléphone, il téléchargera la configuration et contactera ensuite CAPF afin de mettre à jour le LSC. Après la mise à jour du LSC, le téléphone s'enregistrera comme il se doit. Cela fonctionne tant qu'un nouveau certificat CAPF se trouve dans le fichier ITL et que le téléphone a téléchargé et fait confiance au certificat qui l'a signé (callmanager.pem).

Régénération du CallManager

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

```
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.
```

Régénération de l'IPsec

Lors de la régénération, le certificat IPsec se télécharge automatiquement vers ipsec-trust.

```
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.
```

Régénération de Tomcat

Lors de la régénération, le certificat Tomcat se télécharge automatiquement vers tomcat-trust.

```
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.
```

Régénération du TVS

```
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 à quoi vous attendre

Lorsque vous régénérez des certificats via l'interface de ligne de commande, vous êtes invité à vérifier les modifications effectuées. Entrez « Yes » puis appuyez sur « Enter ».

```
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.
```

Supprimer des certificats avec l'interface de ligne de commande

Suppression des certificats CAPF-trust

```
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.
```

Suppression des certificats CallManager-trust

```
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.
```

Suppression des certificats ipsec-trust

```
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.
```

Enlever les certificats Tomcat-trust

```
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.
```

Suppression des certificats TVS-trust

```
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.
```

Régénérer les certificats avec l'interface graphique Web

Régénération du CAPF

Lors de la régénération, le certificat CAPF se télécharge automatiquement dans CAPF-trust et CallManager-trust. De plus, le certificat CAPF a toujours un nom unique, de sorte que les certificats du CAPF utilisés précédemment seront conservés 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.
```

Régénération du CallManager

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

```
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.
```

Régénération de l'IPsec

Lors de la régénération, le certificat IPsec se télécharge automatiquement vers ipsec-trust.

```
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.
```

Régénération de Tomcat

Lors de la régénération, le certificat Tomcat se télécharge automatiquement vers tomcat-trust.

```
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.
```

Régénération du TVS

```
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.
```

Supprimer des certificats via l’interface graphique 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 la régénération/suppression des certificats

Une fois qu'un certificat a été régénéré d'un magasin ou supprimé, le service visé doit être redémarré pour recevoir les modifications.

Magasin	Service à redémarrer	Comment
Tomcat	Tomcat	CLI : utils service restart Cisco Tomcat GUI de Web : Cisco Unified Serviceability > Outils > Centre contrôle – Services de fonctionnalités > (sélectionner un serv > sélectionner « Cisco CallManager » > Redémarrer
CallManager	CallManager; TFTP ; CTIManager	GUI de Web : Cisco Unified Serviceability > Outils > Centre contrôle – Services de fonctionnalités > (sélectionner un serv > sélectionner « Cisco Tftp » > Redémarrer GUI de Web : Utilité > Tools > Control Center de Cisco Unifi La caractéristique entretient > (serveur choisi) > « Cisco choi CTIManager » > reprise
CAPF	CAPF (seulement sur le serveur diffuseur)	GUI de Web : Cisco Unified Serviceability > Outils > Centre contrôle – Services de fonctionnalités > (sélectionner un serv > sélectionner « Cisco Certificate Authority Proxy Function » Redémarrer
TVS	Trust Verification Service (sur le serveur visé)	GUI de Web : Cisco Unified Serviceability > Outils > Centre c contrôle – Services de fonctionnalités > (sélectionner un serv > sélectionner « Cisco Trust Verification Service » > Redéma
ipsec	Cisco DRF Local (sur tous les nœuds); Cisco DRF Master (sur le serveur diffuseur)	CLI : utils service restart Cisco DRF Local CLI : utils service restart Cisco DRF Master

Installer/mettre à jour LSC sur les téléphones

Si le certificat CAPF a été régénéré, les certificats LSC pour tous les téléphones de la grappe doivent être mis à jour avec un LSC signé par le nouveau certificat CAPF.

1. Choisissez « **CUCM Serviceability » > « Service Activation** ». Activez la fonction « Cisco CTL Provider » et « Cisco Certificate Authority Proxy Function » sur le serveur diffuseur.
2. Dans CCMAdmin de CUCM, choisissez « **Device > Phone** ». Choisissez le téléphone IP sur lequel vous voulez verser un LSC.
3. Dans la page de configuration du périphérique, sous « Certificate Operation », choisissez « **Install / Upgrade » > « By Null String »**.
4. Sauvegardez la configuration du téléphone dans CCMAdmin et choisissez « **Apply Config** ».

Si le téléphone a des problèmes avec l'installation du LSC, effectuez ces actions sur le téléphone :

Lorsque le téléphone se réinitialise, rendez-vous sur le téléphone physique et choisissez Paramètres **> (6) Configuration de Sécurité > (4) LSC > * * #** (cette opération déverrouille le GUI et permet de nous pour continuer à l' étape suivante) **> mettre à Jour** (mise à jour ne seront pas visibles jusqu' à ce que vous effectuez le étape précédente) **> submit (soumettre)** .

N'assignez aucun certificat à un téléphone, sauf s'il s'agit d'un téléphone sans fil (7921/25). Les

téléphones sans fil utilisent des autorités de certification tierces pour s’authentifier.

Conclusion

Si vous rencontrez un problème ou avez besoin d’aide avec cette procédure, communiquez avec le Centre d’assistance technique Cisco (TAC). Dans ce cas, gardez votre sauvegarde DRF disponible, car elle sera utilisée en dernier recours afin de rétablir le service si le TAC n’est pas en mesure de le faire par d’autres méthodes.