Améliorations ITL d'Unified Communications Manager dans la version 10.0(1)

Contenu

Introduction

Ce document décrit une nouvelle caractéristique dans la version 10.0(1) de Cisco Unified Communications Manager (CUCM) qui active la remise en vrac des fichiers de la liste de confiance d'identité (ITL) sur des Téléphones IP de Cisco Unified. La caractéristique de remise ITL en vrac est utilisée quand les téléphones ne font confiance plus au signataire de fichier ITL et ne peuvent pas également authentifier le fichier ITL équipé par le service TFTP localement ou d'utilisation du service de vérification de confiance (TV).

Fond

La capacité d'entasser en vrac des fichiers ITL de remise empêche la nécessité d'exécuter une ou plusieurs de ces étapes pour rétablir la confiance entre les Téléphones IP et les serveurs CUCM.

- Restauration d'un de sauvegarde afin de télécharger un vieux fichier ITL au lequel les téléphones font confiance
- Changez les téléphones afin d'utiliser un serveur différent TFTP
- Supprimez le fichier ITL du téléphone manuellement par le menu Settings
- Réinitialisation aux paramètres d'usine les configurations de téléphone en cas de sorte que l'accès soit désactivé afin d'effacer l'ITL

Cette caractéristique n'est pas destinée pour déplacer des téléphones entre les batteries ; pour cette tâche, utilisez une des méthodes décrites en migrant des Téléphones IP entre les batteries

avec des fichiers CUCM 8 et ITL. L'exécution de remise ITL est utilisée pour rétablir seulement la confiance entre les Téléphones IP et la batterie CUCM quand ils ont perdu leurs points de confiance.

Une autre caractéristique liée à la sécurité disponible dans la version 10.0(1) CUCM qui n'est pas couverte dans ce document est la liste de confiance de Tokenless Certficate (CTL). Le Tokenless CTL remplace les jetons de degré de sécurité du matériel USB par un jeton de logiciel utilisé afin d'activer le cryptage sur les serveurs et des points finaux CUCM. Pour information les informations complémentaires, référez-vous au degré de sécurité de téléphone IP et au document CTL (liste de confiance de certificat).

Les informations complémentaires sur les fichiers et la Sécurité ITL par défaut peuvent être trouvées dans la Sécurité de gestionnaire de transmissions par le document de par défaut et d'exécution et de dépannage ITL.

Symptômes du problème

Quand les téléphones sont dans un état **verrouillé** ou **non approuvé**, ils ne reçoivent pas le fichier ITL ou la configuration TFTP fournie par le service TFTP. Aucune modification de configuration qui est contenue dans le fichier de configuration TFTP n'est appliquée au téléphone. Quelques exemples des configurations qui sont contenues dans le fichier de configuration TFTP sont :

- Configurations Access
- Accès au Web
- Protocole Secure Shell (SSH) Access
- Fonction Switched Port Analyzer (SPAN) au port PC

Si l'un de ces configurations sont changées pour un téléphone à la page de l'admin CCM et, après que le téléphone soit remis à l'état initial, les modifications ne le prenez pas effet, le téléphone ne pourrait pas faire confiance au serveur TFTP. Un autre symptôme commun est quand vous accédez au répertoire d'entreprise ou d'autres services de téléphonie, les affichages **non trouvés d'hôte de** message. Afin de vérifier que le téléphone est dans un état verrouillé ou non approuvé, vérifiez les messages d'état du téléphone du téléphone lui-même ou la page Web de téléphone afin de voir si une **mise à jour de liste de confiance manquait des** affichages de message. **La mise à jour ITL a manqué** message est un indicateur que le téléphone est dans un état verrouillé ou non approuvé parce qu'il n'a pas authentifié la liste de confiance avec son ITL de courant et ne l'a pas authentifiée avec des TV.

La mise à jour de liste de confiance a manqué message peut être vue du téléphone lui-même si vous naviguez vers des **configurations > l'état > des messages d'état** :

La mise à jour de liste de confiance a manqué message peut également être vue de la page Web de téléphone des **messages d'état** comme affiché ici :

Solution - Remise en vrac ITL

La version 10.0(1) CUCM utilise une clé supplémentaire qui peut être utilisée afin de rétablir la confiance entre les téléphones et les serveurs CUCM. Cette nouvelle clé est la clé de reprise ITL. La clé de reprise ITL est créée pendant l'installer ou la mise à jour. Cette clé de reprise ne change pas quand l'adresse Internet change, des DN change, ou d'autres modifications sont exécutées

qui pourraient mener aux problèmes où les téléphones entrent dans un état où ils ne font confiance plus au signataire de leurs fichiers de configuration.

La nouvelle commande CLI de **remise ITL d'utils** peut être utilisée afin de rétablir la confiance entre un téléphone ou des téléphones et le service TFTP sur CUCM quand les téléphones sont dans un état où la **mise à jour de liste de confiance a manqué** message est vus. La commande de **remise ITL d'utils** :

1. Prend le fichier ITL de courant du noeud d'éditeur, élimine la signature du fichier ITL, et signe le contenu du fichier ITL de nouveau avec la clé privée de reprise ITL.
2. Copie automatiquement le nouveau fichier ITL sur les répertoires TFTP sur tous les Noeuds actifs TFTP dans la batterie.
3. Redémarre automatiquement les services TFTP sur chaque noeud où le TFTP fonctionne.

L'administrateur doit alors remettre à l'état initial tous les téléphones. La remise fait demander les téléphones le fichier ITL sur l'amorce du serveur TFTP et le fichier ITL que le téléphone reçoit est signé par la clé d'ITLRecovery au lieu de la clé **privée callmanager.pem**. Il y a deux options d'exécuter une ITL remise à l'état initial : **localkey de remise d'**utilsitl **et remotekey de remise d'**utilsitl**.** La commande de remise ITL peut seulement être exécutée de l'éditeur. Si vous émettez une ITL remise à l'état initial d'un abonné, elle a comme conséquence le Thisis **pas un message de noeud de Publisher**. Des exemples de chaque commande sont détaillés dans les sections suivantes.

ITLRecovery avec la clé locale de reprise

L'option de localkey utilise la clé privée de reprise ITL contenue dans le fichier ITLRecovery.p12 actuel sur le disque dur de Publisher comme le nouveau signataire de fichier ITL.

```
admin:utils itl reset localkey
Enter CCM Administrator password :

Locating active Tftp servers in the cluster.....

Following is the list of Active tftp servers in the cluster

['test10pub', 'test10sub']
The reset ITL file was generated successfully


Transferring new reset ITL file to the TFTP server nodes in the cluster.........

Restarting Cisco Tftp service on host test10pub
Cisco Tftp service restarted on host test10pub
Successfully transferred reset ITL to node test10sub

Restarting Cisco Tftp service on host test10sub
Cisco Tftp service restarted on host test10sub
```

ITLRecovery avec la clé distante de reprise

L'option de remotekey permet le serveur externe de SFTP dont le fichier ITLRecovery.p12 a été enregistré pour être spécifié.

```
admin:utils itl reset remotekey joemar2-server.cisco.com joemar2
/home/joemar2/ITLRecovery.p12
```

```
Enter Sftp password :Processing token in else 0 tac
coutn is 1
Processing token in else 0 tac
coutn is 1



Enter CCM Administrator password :

Locating active Tftp servers in the cluster.....

Following is the list of Active tftp servers in the cluster

['test10pub', 'test10sub']
The reset ITL file was generated successfully


Transferring new reset ITL file to the TFTP server nodes in the cluster.........

Restarting Cisco Tftp service on host test10pub
Cisco Tftp service restarted on host test10pub
Successfully transferred reset ITL to node test10sub

Restarting Cisco Tftp service on host test10sub
Cisco Tftp service restarted on host test10sub
```

> Remarque: Si une remise ITL est faite avec l'option de remotekey, le localkey (sur le fichier-disque) sur l'éditeur est remplacé par le remotekey.

Vérifiez le signataire en cours avec la commande « ITL d'exposition »

Si vous visualisez le fichier ITL avec la commande **ITL d'exposition** avant que vous émettiez une ITL remettez à l'état initial la commande, il prouve que l'ITL contient une entrée de *<publisher_hostname>* **ITLRECOVERY_**. Chaque fichier ITL qui est servi par n'importe quel serveur TFTP dans la batterie contient cette entrée de reprise ITL de l'éditeur. La sortie de la commande **ITL d'exposition** est prise de l'éditeur dans cet exemple. Le jeton utilisé afin de signer l'ITL est en gras :

```
admin:show itl
The checksum value of the ITL file:
b331e5bfb450926e816be37f2d8c24a2(MD5)
9d7da73d16c1501b4d27dc1ed79211f390659982(SHA1)


Length of ITL file: 5302
The ITL File was last modified on Wed Feb 26 10:24:27 PST 2014

Parse ITL File
----------------

Version: 1.2
HeaderLength: 324 (BYTES)

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
3 SIGNERID 2 139
4 SIGNERNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
5 SERIALNUMBER 16 61:40:52:E9:1E:E9:7C:77:9B:7B:5E:81:0A:B1:46:A5
6 CANAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
```

```
7 SIGNATUREINFO 2 15
8 DIGESTALGORTITHM 1
9 SIGNATUREALGOINFO 2 8
10 SIGNATUREALGORTITHM 1
11 SIGNATUREMODULUS 1
12 SIGNATURE 128
8f d4 0 cb a8 23 bc b0
f 75 69 9e 25 d1 9b 24
49 6 ae d0 68 18 f6 4
52 f8 1d 27 7 95 bc 94
d7 5c 36 55 8d 89 ad f4
88 0 d7 d0 db da b5 98
12 a2 6f 2e 6a be 9a dd
da 38 df 4f 4c 37 3e f6
ec 5f 53 bf 4b a9 43 76
35 c5 ac 56 e2 5b 1b 96
df 83 62 45 f5 6d 0 2f
c d1 b8 49 88 8d 65 b4
34 e4 7c 67 5 3f 7 59
b6 98 16 35 69 79 8f 5f
20 f0 42 5b 9b 56 32 2b
c0 b7 1a 1e 83 c9 58 b
14 FILENAME 12
15 TIMESTAMP 4

ITL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1115
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 61:40:52:E9:1E:E9:7C:77:9B:7B:5E:81:0A:B1:46:A5
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 684 01 9C 4C 3D 27 D7 4D 82 CB B1 84 84 D4 2A 63 9F 71 78 BE A9
(SHA1 Hash HEX)
This etoken was used to sign the ITL file.

ITL Record #:2
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1115
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 TFTP
5 ISSUERNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 61:40:52:E9:1E:E9:7C:77:9B:7B:5E:81:0A:B1:46:A5
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 684 01 9C 4C 3D 27 D7 4D 82 CB B1 84 84 D4 2A 63 9F 71 78 BE A9
(SHA1 Hash HEX)
ITL Record #:3
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 439
2 DNSNAME 2
3 SUBJECTNAME 49 CN=CAPF-75638ad9;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 CAPF
5 ISSUERNAME 49 CN=CAPF-75638ad9;OU=tac;O=cisco;L=rtp;ST=nc;C=US
```

```
6 SERIALNUMBER 16 42:BF:37:77:9B:16:AF:1C:D2:30:88:C2:17:24:9D:AA
7 PUBLICKEY 140
8 SIGNATURE 128
11 CERTHASH 20 BB C3 4A 1D DE 17 39 C5 36 1A 15 6B F0 65 FE BE D1 E6 19 03
12 HASH ALGORITHM 1 SHA-1

ITL Record #:4
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 455
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 76:59:84:D8:B7:30:60:63:36:E5:C7:B6:A7:DD:B9:D6
7 PUBLICKEY 140
8 SIGNATURE 128
11 CERTHASH 20 7A BF CE B6 BE E2 06 02 74 D9 EB AE 58 48 52 93 7A 1E A5 55
12 HASH ALGORITHM 1 SHA-1

ITL Record #:5
----
BYTEPOS TAG LENGTH VALUE


------- --- ------ -----
1 RECORDLENGTH 2 1141
2 DNSNAME 2
3 SUBJECTNAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;
ST=nc;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;
ST=nc;C=US
6 SERIALNUMBER 16 6E:3F:65:C2:97:B3:E0:1F:E7:42:81:AB:52:CC:55:DC
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 692 CD C7 4A 39 87 87 52 FA B0 89 0C 28 AB CB 36 32 EB 87 16 DC
(SHA1 Hash HEX)
This etoken was not used to sign the ITL file.

ITL Record #:6
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 713
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10sub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 57 CN=test10sub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 67:D1:A1:9E:F8:AB:91:E6:C0:A6:10:35:26:30:EE:02
7 PUBLICKEY 270
8 SIGNATURE 256
11 CERTHASH 20 AF 28 89 16 F9 94 E6 62 A3 65 C2 88 3B 94 08 1C 66 7C 49 C9
12 HASH ALGORITHM 1 SHA-1

The ITL file was verified successfully.
```

Vérifiez que la clé d'ITLRecovery est utilisée

Si vous visualisez le fichier ITL avec la commande **ITL d'exposition** après que vous exécutiez une remise ITL, elle prouve que l'entrée d'ITLRecovery a signé l'ITL comme affiché ici. L'ITLRecovery

reste le signataire de l'ITL jusqu'à ce que le TFTP soit redémarré, quand le **callmanager.pem ou le** certificat TFTP est utilisé afin de signer l'ITL de nouveau.

```
admin:show itl
The checksum value of the ITL file:
c847df047cf5822c1ed6cf376796653d(MD5)
3440f94f9252e243c99506b4bd33ea28ec654dab(SHA1)


Length of ITL file: 5322
The ITL File was last modified on Wed Feb 26 10:34:46 PST 2014<

Parse ITL File
----------------

Version: 1.2
HeaderLength: 344 (BYTES)

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
3 SIGNERID 2 157
4 SIGNERNAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
5 SERIALNUMBER 16 6E:3F:65:C2:97:B3:E0:1F:E7:42:81:AB:52:CC:55:DC
6 CANAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
7 SIGNATUREINFO 2 15
8 DIGESTALGORTITHM 1
9 SIGNATUREALGOINFO 2 8
10 SIGNATUREALGORTITHM 1
11 SIGNATUREMODULUS 1
12 SIGNATURE 128
58 ff ed a ea 1b 9a c4
e 75 f0 2b 24 ce 58 bd
6e 49 ec 80 23 85 4d 18
8b d0 f3 85 29 4b 22 8f
b1 c2 7e 68 ee e6 5b 4d
f8 2e e4 a1 e2 15 8c 3e
97 c3 f0 1d c0 e 6 1b
fc d2 f3 2e 89 a0 77 19
5c 11 84 18 8a cb ce 2f
5d 91 21 57 88 2c ed 92
a5 8f f7 c 0 c1 c4 63
28 3d a3 78 dd 42 f0 af
9d f1 42 5e 35 3c bc ae
c 3 df 89 9 f9 ac 77
60 11 1f 84 f5 83 d0 cc
14 FILENAME 12
15 TIMESTAMP 4

ITL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1115
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 61:40:52:E9:1E:E9:7C:77:9B:7B:5E:81:0A:B1:46:A5
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 684 01 9C 4C 3D 27 D7 4D 82 CB B1 84 84 D4 2A 63 9F 71 78 BE A9
(SHA1 Hash HEX)
This etoken was not used to sign the ITL file.
```

```
ITL Record #:2
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1115
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 TFTP
5 ISSUERNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 61:40:52:E9:1E:E9:7C:77:9B:7B:5E:81:0A:B1:46:A5
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 684 01 9C 4C 3D 27 D7 4D 82 CB B1 84 84 D4 2A 63 9F 71 78 BE A9
(SHA1 Hash HEX)

ITL Record #:3
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 439
2 DNSNAME 2
3 SUBJECTNAME 49 CN=CAPF-75638ad9;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 CAPF
5 ISSUERNAME 49 CN=CAPF-75638ad9;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 42:BF:37:77:9B:16:AF:1C:D2:30:88:C2:17:24:9D:AA
7 PUBLICKEY 140
8 SIGNATURE 128
11 CERTHASH 20 BB C3 4A 1D DE 17 39 C5 36 1A 15 6B F0 65 FE BE D1 E6 19 03
12 HASH ALGORITHM 1 SHA-1

ITL Record #:4
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 455
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 76:59:84:D8:B7:30:60:63:36:E5:C7:B6:A7:DD:B9:D6
7 PUBLICKEY 140
8 SIGNATURE 128
11 CERTHASH 20 7A BF CE B6 BE E2 06 02 74 D9 EB AE 58 48 52 93 7A 1E A5 55
12 HASH ALGORITHM 1 SHA-1

ITL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1141
2 DNSNAME 2
3 SUBJECTNAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 6E:3F:65:C2:97:B3:E0:1F:E7:42:81:AB:52:CC:55:DC
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 692 CD C7 4A 39 87 87 52 FA B0 89 0C 28 AB CB 36 32 EB 87 16 DC
(SHA1 Hash HEX)
This etoken was used to sign the ITL file.

ITL Record #:6
----
```

```
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 713
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10sub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 57 CN=test10sub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 67:D1:A1:9E:F8:AB:91:E6:C0:A6:10:35:26:30:EE:02
7 PUBLICKEY 270
8 SIGNATURE 256
11 CERTHASH 20 AF 28 89 16 F9 94 E6 62 A3 65 C2 88 3B 94 08 1C 66 7C 49 C9
12 HASH ALGORITHM 1 SHA-1

The ITL file was verified successfully.
```

Améliorations pour diminuer la possibilité de téléphones perdant la confiance

En plus de la capacité de remise ITL, la version 10.0(1) CUCM inclut les caractéristiques d'administrateur qui aident à empêcher des téléphones d'écrire un état non approuvé. La confiance deux dirige le téléphone a sont le certificat TV (**TVS.pem) et le** certificat TFTP (callmanager.pem**). Dans l'**environnement le plus simple avec seulement un serveur CUCM, si un administrateur régénère le callmanager.pemcertificate et le certificat TVS.pem un juste après des autres, les remises de téléphone et lors du démarrage affiche la **mise à jour de** liste de confiance **ont manqué message. Même** avec une remise de périphérique automatique envoyée de CUCM au téléphone dû à un certificat contenu dans l'ITL qui est régénérée, le téléphone peut entrer dans un état où il ne fait pas confiance à CUCM.

Afin d'aider à empêcher le scénario où de plusieurs Certificats sont régénérés en même temps (typiquement modification d'adresse Internet ou des modifications de nom de domaine de DN), CUCM a maintenant un temporisateur d'attente. Quand un certificat est régénéré, CUCM empêche l'administrateur de régénérer un autre certificat sur le même noeud dans un délai de cinq minutes de la régénération précédente de certificat. Ce processus cause les téléphones d'être remis à l'état initial en régénérant le premier certificat, et ils devraient être sauvegardent et se sont enregistrés avant que le prochain certificat soit régénéré.

Indépendamment quel certificat est généré d'abord, le téléphone a sa méthode secondaire pour authentifier des fichiers. Des détails supplémentaires au sujet de ce processus peuvent être trouvés dans la Sécurité de gestionnaire de transmissions par défaut et exécution et dépannage ITL.

Cette sortie affiche à une situation où CUCM empêche l'administrateur de régénérer un autre certificat dans un délai de cinq minutes d'une régénération précédente de certificat comme visualisées du CLI :

```
admin:set cert regen CallManager

WARNING: This operation will overwrite any CA signed certificate
previously imported for CallManager
Proceed with regeneration (yes|no)? yes


Successfully Regenerated Certificate for CallManager.
Please do a backup of the server as soon as possible. Failure to do
so can stale the cluster in case of a crash.
You must restart services related to CallManager for the regenerated
```

```
certificates to become active.

admin:set cert regen TVS

CallManager certificate was modified in the last 5 minutes. Please re-try
regnerating TVS certificate at a later time
```

Le même message peut être vu de la page du système d'exploitation de gestion (de SYSTÈME D'EXPLOITATION) comme affiché ici :

La clé de reprise ITL d'éditeur est la seule en service par la batterie entière, quoique chaque noeud ait son propre certificat d'ITLRecovery fourni au nom commun (NC) du ***name> de <node d'*1TLRecovery_**. La clé d'ITLRecovery d'éditeur est la seule utilisée dans les fichiers ITL pour la batterie entière comme vu de la commande **ITL d'exposition**. C'est pourquoi la seule entrée de ***<hostname> d'*1TLRecovery_** vue dans un fichier ITL contient l'adresse Internet de l'éditeur.

Si l'adresse Internet de l'éditeur est changée, l'entrée d'ITLRecovery dans l'ITL continue à afficher la vieille adresse Internet de l'éditeur. Ceci est fait intentionnellement parce que le fichier d'ITLRecovery devrait ne jamais changer pour assurer à la confiance de téléphones toujours la reprise ITL.

Ceci s'applique pour quand des noms de domaine sont changés aussi ; le nom de domaine initial est vu dans l'entrée d'ITLRecovery afin de s'assurer que la clé de reprise ne change pas. Le seul cas où le certificat d'ITLRecovery devrait changer est quand il expire en raison de la validité de cinq ans et doit être régénéré.

Les keypairs de reprise ITL peuvent être régénérés avec le CLI ou la page de gestion de SYSTÈME D'EXPLOITATION. Des Téléphones IP ne sont pas remis à l'état initial quand le certificat d'ITLRecovery est régénéré sur l'éditeur ou les abonnés l'uns des. Une fois que le certificat d'ITLRecovery a été régénéré, le fichier ITL ne met pas à jour jusqu'à ce que le service TFTP soit redémarré. Après que la régénération de certificat d'ITLRecovery sur l'éditeur, redémarrent le service TFTP sur chaque noeud qui dirige le service TFTP dans la batterie afin de mettre à jour l'entrée d'ITLRecovery dans le fichier ITL avec le nouveau certificat. La dernière étape est de remettre à l'état initial tous les périphériques de **System > Enterprise Parameters** et d'utiliser le bouton de réinitialisation afin de faire à tout le téléchargement de périphériques le nouveau fichier ITL qui contient le nouveau certificat d'ITLRecovery.

Sauvegardez la reprise ITL

La clé de reprise ITL est exigée afin de récupérer des téléphones quand ils entrent dans un état non approuvé. En raison de ceci, de nouvelles alertes de l'outil de suivi en temps réel (RTMT) sont générées quotidiennement jusqu'à ce que la clé de reprise ITL soit sauvegardée. Une sauvegarde du système de Reprise sur sinistre (jeu rouleau-tambour) ne suffit pas pour arrêter les alertes. Bien qu'une sauvegarde soit recommandée afin de sauvegarder la clé de reprise ITL, une sauvegarde manuelle du fichier principal est aussi bien nécessaire.

Afin de sauvegarder la clé de reprise, la procédure de connexion au CLI de l'éditeur et introduire le **fichier obtiennent la** commande du **tftp ITLRecovery.p12**. Un serveur de SFTP est nécessaire afin de sauvegarder le fichier à comme affiché ici. Les Noeuds d'abonné n'ont pas un fichier d'images Avant ITL, ainsi si vous émettez le **fichier obtiennent la** commande du **tftp ITLRecovery.p12** sur un abonné, il ont comme conséquence le **fichier non trouvé**.

```
admin:file get tftp ITLRecovery.p12
```

```
Please wait while the system is gathering files info ...done.
Sub-directories were not traversed.
Number of files affected: 1
Total size in Bytes: 1709
Total size in Kbytes: 1.6689453
Would you like to proceed [y/n]? y
SFTP server IP: joemar2-server.cisco.com
SFTP server port [22]:
User ID: joemar2
Password: *************

Download directory: /home/joemar2/

The authenticity of host 'joemar2-server.cisco.com (172.18.172.254)' can't be
established.
RSA key fingerprint is 2c:8f:9b:b2:ff:f7:a6:31:61:1b:bc:95:cc:bc:ba:bd.
Are you sure you want to continue connecting (yes/no)? yes
.
Transfer completed.
Downloading file: /usr/local/cm/tftp/ITLRecovery.p12
```

Jusqu'à ce que la sauvegarde manuelle soit exécutée du CLI afin de sauvegarder le fichier ITLRecovery.p12, un avertissement est imprimé dans le CiscoSyslog (journal de l'observateur d'événements) chaque jour comme affiché ici. Un email quotidien pourrait également être reçu jusqu'à ce que la sauvegarde manuelle soit exécutée si la notification électronique est activée de la page de gestion de SYSTÈME D'EXPLOITATION, **Sécurité > moniteur de certificat**.

Tandis qu'une sauvegarde jeu rouleau-tambour contient l'ITLRecovery, elle est recommandée d'enregistrer toujours le fichier ITLRecovery.p12 dans un emplacement sûr au cas où les fichiers de sauvegarde seraient perdus ou corrompus ou afin d'avoir l'option de remettre à l'état initial le fichier ITL sans nécessité de restaurer d'une sauvegarde. Si vous avez le fichier ITLRecovery.p12 de l'éditeur enregistré, il permet également l'éditeur à reconstruire sans sauvegarde avec l'utilisation l'option de restauration jeu rouleau-tambour de restaurer la base de données d'un susbcriber et de rétablir la confiance entre les téléphones et les serveurs CUCM en remettant à l'état initial l'ITL avec l'option de **remotekey de remise ITL d'utils**.

Souvenez-vous que si l'éditeur est reconstruit, le mot de passe de Sécurité de batterie devrait être identique que l'éditeur d'où le fichier ITLRecovery.p12 a été pris parce que le fichier ITLRecovery.p12 est protégé par mot de passe avec un mot de passe basé hors fonction du mot de passe de Sécurité de batterie. Pour cette raison, si le mot de passe de Sécurité de batterie est changé, l'alerte RTMT qui indique que le fichier ITLRecovery.p12 n'a pas été sauvegardé est remise à l'état initial et déclenche le journal jusqu'à ce que le nouveau fichier ITLRecovery.p12 soit enregistré avec le **fichier obtiennent la** commande du **tftp ITLRecovery.p12**.

Vérifiez

La caractéristique de remise ITL en vrac fonctionne seulement si les téléphones ont une ITL installée qui contient l'entrée d'ITLRecovery. Afin de vérifier que le fichier ITL installé aux téléphones contient l'entrée d'ITLRecovery, sélectionnez la commande **ITL d'exposition du** CLI sur chacun des serveurs TFTP de trouver la somme de contrôle du fichier ITL. La sortie de la commande **ITL d'exposition** affiche la somme de contrôle :

```
admin:show itl
The checksum value of the ITL file:
b331e5bfb450926e816be37f2d8c24a2(MD5)
9d7da73d16c1501b4d27dc1ed79211f390659982(SHA1)
```

La somme de contrôle est différente sur chaque serveur TFTP parce que chaque serveur a son propre **certificat callmanager.pem** dans son fichier ITL. La somme de contrôle ITL de l'ITL installée au téléphone peut être trouvée si vous visualisez l'ITL au téléphone elle-même sous les configurations **> la liste de configuration de sécurité > de confiance, de la** page Web de téléphone, ou de l'alarme de DeviceTLInfo signalée par les téléphones qui exécutent un plus nouveau micrologiciel.

La plupart des téléphones qui exécutent l'état de version 9.4(1) ou ultérieures de micrologiciels les informations parasites SHA1 de leur ITL à CUCM avec l'alarme de DeviceTLInfo. Les informations envoyées par le téléphone peuvent être en cas visualiseur visualisé - journal d'application de RTMT et comparé aux informations parasites SHA1 des informations parasites ITL des serveurs TFTP que les téléphones les utilisent afin de trouver tous les téléphones qui n'ont pas l'ITL de courant installée, qui contient l'entrée d'ITLRecovery.

Mises en garde

- CSCun18578 - La remise localkey/remotekey ITL échoue dans certains scénarios
- CSCun19112 - Erreur de remotekey de remise ITL dans le type d'authentification erronée de SFTP