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

Contenu

Introduction

Ce document décrit une nouvelle fonctionnalité de Cisco Unified Communications Manager (CUCM) Version 10.0(1) qui active la réinitialisation en masse des fichiers de la liste de confiance d'identité (ITL) sur les téléphones IP Cisco Unified. La fonctionnalité de réinitialisation ITL en bloc est utilisée lorsque les téléphones ne font plus confiance au signataire du fichier ITL et ne peuvent pas non plus authentifier le fichier ITL fourni localement par le service TFTP ou avec l'utilisation du service de vérification de confiance (TVS).

Fond

La possibilité de réinitialiser en bloc les fichiers ITL évite d'effectuer une ou plusieurs de ces étapes pour rétablir la confiance entre les téléphones IP et les serveurs CUCM.

- Restaurer à partir d'une sauvegarde afin de télécharger un ancien fichier ITL approuvé par les téléphones
- Modifier les téléphones afin d'utiliser un autre serveur TFTP
- Supprimer manuellement le fichier ITL du téléphone via le menu Paramètres
- Réinitialisez le téléphone en usine dans les paramètres d'événement de sorte que l'accès soit désactivé afin d'effacer l'ITL

Cette fonctionnalité n'est pas destinée à déplacer les téléphones entre les clusters ; pour cette tâche, utilisez l'une des méthodes décrites dans la section Migration des téléphones IP entre les

clusters avec CUCM 8 et les fichiers ITL. L'opération de réinitialisation ITL est utilisée uniquement pour rétablir la confiance entre les téléphones IP et le cluster CUCM lorsqu'ils ont perdu leurs points de confiance.

Une autre fonctionnalité liée à la sécurité disponible dans CUCM version 10.0(1) qui n'est pas couverte dans ce document est la liste CTL (Tokenless Certficate Trust List). La CTL sans jeton remplace les jetons de sécurité USB matériels par un jeton logiciel utilisé afin d'activer le chiffrement sur les serveurs et les terminaux CUCM. Pour plus d'informations, consultez le document Sécurité des téléphones IP et CTL (Certificate Trust List).

Des informations supplémentaires sur les fichiers ITL et la sécurité par défaut sont disponibles dans le document Communications Manager Security By Default et ITL Operation and Troubleshooting.

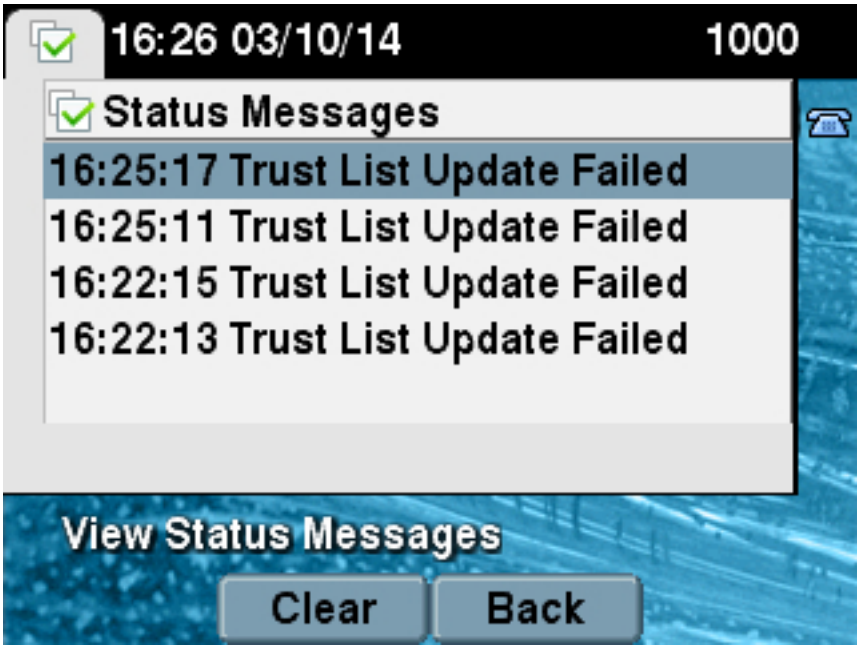
Symptômes du problème

Lorsque les téléphones sont dans un état **verrouillé** ou **non approuvé**, ils n'acceptent pas le fichier ITL ou la configuration TFTP fournie par le service TFTP. Aucune modification de configuration contenue dans le fichier de configuration TFTP n'est appliquée au téléphone. Voici quelques exemples de paramètres contenus dans le fichier de configuration TFTP :

- Accès aux paramètres
- Accès Web
- Accès SSH (Secure Shell)
- SPAN (Switched Port Analyzer) vers port PC

Si l'un de ces paramètres est modifié pour un téléphone sur la page CCM Admin et, après la réinitialisation du téléphone, les modifications ne prennent pas effet, le téléphone risque de ne pas faire confiance au serveur TFTP. Un autre symptôme courant est que lorsque vous accédez au répertoire d'entreprise ou à d'autres services téléphoniques, le message **Hôte introuvable** s'affiche. Afin de vérifier que le téléphone est verrouillé ou non approuvé, vérifiez les messages d'état du téléphone à partir du téléphone lui-même ou de la page Web du téléphone afin de voir si un message **Échec de mise à jour de la liste de confiance** s'affiche. Le message **Échec de la mise à jour ITL** indique que le téléphone est verrouillé ou non approuvé car il n'a pas pu authentifier la liste d'approbation avec son ITL actuel et ne l'a pas authentifié avec TVS.

Le message **Échec de la mise à jour de la liste de confiance** peut être vu à partir du téléphone lui-même si vous accédez à **Paramètres > État > Messages d'état** :



Le message **Échec de la mise à jour de la liste de confiance** peut également être vu à partir de la page Web du téléphone à partir des **messages d'état** comme indiqué ici :

Solution - Réinitialisation ITL en masse

CUCM version 10.0(1) utilise une clé supplémentaire qui peut être utilisée pour rétablir la confiance entre les téléphones et les serveurs CUCM. Cette nouvelle clé est la clé de récupération ITL. La clé de récupération ITL est créée lors de l'installation ou de la mise à niveau. Cette clé de récupération ne change pas lorsque des modifications de nom d'hôte, de DNS ou d'autres modifications sont effectuées qui peuvent entraîner des problèmes lorsque les téléphones se trouvent dans un état où ils ne font plus confiance au signataire de leurs fichiers de configuration.

La nouvelle commande CLI **utils itl reset** peut être utilisée afin de rétablir la confiance entre un ou plusieurs téléphones et le service TFTP sur CUCM lorsque les téléphones sont dans un état où le message **Échec de mise à jour de la liste de confiance** est affiché. La commande **utils itl reset** :

1. Prend le fichier ITL actuel du noeud éditeur, retire la signature du fichier ITL et signe à nouveau le contenu du fichier ITL avec la clé privée ITL Recovery.
2. Copie automatiquement le nouveau fichier ITL dans les répertoires TFTP de tous les noeuds TFTP actifs du cluster.
3. Redémarre automatiquement les services TFTP sur chaque noeud où TFTP s'exécute.

L'administrateur doit ensuite réinitialiser tous les téléphones. La réinitialisation entraîne la

demande du fichier ITL au démarrage à partir du serveur TFTP et le fichier ITL reçu par le téléphone est signé par la clé ITLRecovery au lieu de la clé privée **callmanager.pem**. Il existe deux options pour exécuter une réinitialisation ITL : **utils itl reset localkey** et **utils itl reset remotekey**. La commande ITL reset ne peut être exécutée qu'à partir de l'éditeur. Si vous émettez une réinitialisation ITL à partir d'un abonné, le message **Ceci n'est pas un noeud de serveur de publication** s'affiche. Des exemples de chaque commande sont détaillés dans les sections suivantes.

ITLRecovery avec la clé de récupération locale

L'option de clé locale utilise la clé privée de récupération ITL contenue dans le fichier ITLRecovery.p12 présent sur le disque dur Publisher comme 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 de récupération à distance

L'option remotekey permet de spécifier le serveur SFTP externe à partir duquel le fichier ITLRecovery.p12 a été enregistré.

```
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
```

> **Note**: Si une réinitialisation ITL est effectuée avec l'option de touche à distance, la clé locale (sur le fichier disque) de l'éditeur est remplacée par la clé à distance.

Vérifier le signal actuel à l'aide de la commande show itl

Si vous affichez le fichier ITL à l'aide de la commande **show itl** avant d'émettre une commande ITL reset, elle indique que le fichier ITL contient une entrée **ITLRECOVERY_*<publisher_hostname>***. Chaque fichier ITL qui est desservi par un serveur TFTP du cluster contient cette entrée de récupération ITL de la part de l'éditeur. La sortie de la commande **show itl** provient de l'éditeur dans cet exemple. Le jeton utilisé pour 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 ITLRecovery est utilisée

Si vous affichez le fichier ITL à l'aide de la commande **show itl** après avoir effectué une réinitialisation ITL, cela montre que l'entrée ITLRecovery a signé l'ITL comme indiqué ici. ITLRecovery reste le signataire de l'ITL jusqu'au redémarrage du TFTP, au moment où le certificat **callmanager.pem** ou TFTP est utilisé pour signer à nouveau l'ITL.

```
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 réduire la possibilité de perte de confiance des téléphones

Outre la fonctionnalité de réinitialisation ITL, CUCM version 10.0(1) inclut des fonctions d'administrateur qui empêchent les téléphones d'entrer dans un état non approuvé. Les deux points de confiance du téléphone sont le certificat TVS (**TVS.pem**) et le certificat TFTP (**callmanager.pem**). Dans l'environnement le plus simple avec un seul serveur CUCM, si un administrateur régénère le certificat **callmanager.pem** et le certificat **TVS.pem** l'un après l'autre, le téléphone se réinitialise et au démarrage affiche le message **Échec de la mise à jour de la liste de confiance**. Même avec une réinitialisation automatique de périphérique envoyée de CUCM au téléphone en raison d'un certificat contenu dans l'ITL régénéré, le téléphone peut entrer un état dans lequel il ne fait pas confiance à CUCM.

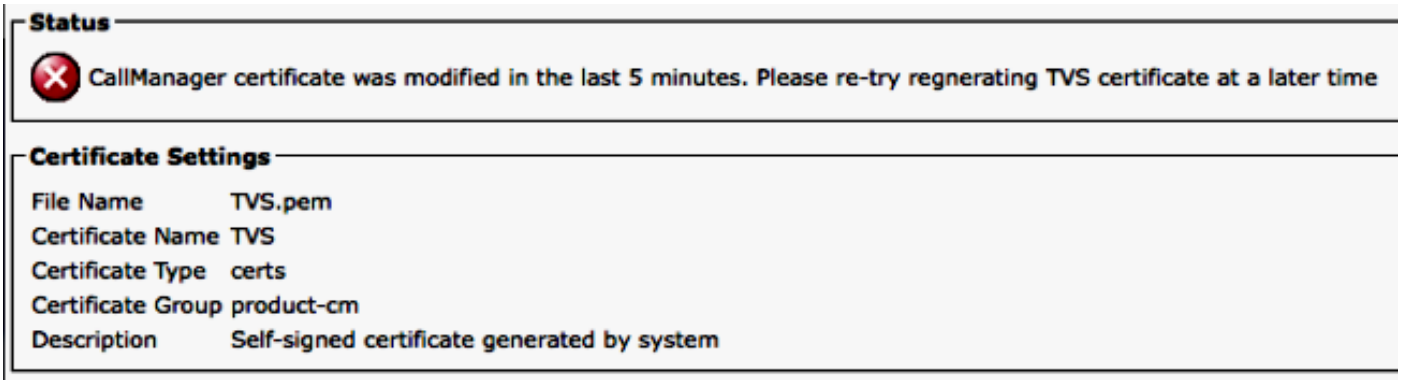
Afin d'empêcher le scénario où plusieurs certificats sont régénérés simultanément (généralement modification du nom d'hôte ou du nom de domaine DNS), CUCM dispose désormais d'un compteur d'attente. Lorsqu'un certificat est régénéré, CUCM empêche l'administrateur de régénérer un autre certificat sur le même noeud dans les cinq minutes qui suivent la régénération du certificat précédent. Ce processus entraîne la réinitialisation des téléphones lors de la régénération du premier certificat, et ils doivent être sauvegardés et enregistrés avant que le certificat suivant ne soit régénéré.

Quel que soit le certificat généré en premier, le téléphone dispose de sa méthode secondaire pour authentifier les fichiers. Des détails supplémentaires sur ce processus sont disponibles dans Communications Manager Security By Default et ITL Operation and Troubleshooting.

Ce résultat montre une situation où CUCM empêche l'administrateur de régénérer un autre certificat dans les cinq minutes suivant la régénération d'un certificat précédent, comme vu à partir de l'interface de ligne de commande :

```
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 s'affiche sur la page d'administration du système d'exploitation (OS), comme indiqué ici :



La clé de récupération ITL de l'éditeur est la seule utilisée par l'ensemble du cluster, même si chaque noeud a son propre certificat ITLRecovery délivré au nom commun (CN) d'**ITLRecovery_*<nom du noeud>***. La clé ITLRecovery de l'éditeur est la seule utilisée dans les fichiers ITL pour l'ensemble du cluster tel qu'il apparaît à partir de la commande **show itl**. C'est pourquoi la seule **entrée ITLRecovery_*<hostname>*** vue dans un fichier ITL contient le nom d'hôte de l'éditeur.

Si le nom d'hôte de l'éditeur est modifié, l'entrée ITLRecovery dans l'ITL continue à afficher l'ancien nom d'hôte de l'éditeur. Ceci est fait intentionnellement parce que le fichier ITLRecovery ne doit jamais changer pour s'assurer que les téléphones font toujours confiance à la récupération ITL.

Cela s'applique également lorsque les noms de domaine sont modifiés ; le nom de domaine d'origine est affiché dans l'entrée ITLRecovery afin de s'assurer que la clé de récupération ne change pas. Le seul moment où le certificat ITLRecovery doit changer est quand il expire en raison de la validité de cinq ans et doit être régénéré.

Les paires de clés de récupération ITL peuvent être régénérées à l'aide de l'interface de ligne de commande ou de la page Administration du système d'exploitation. Les téléphones IP ne sont pas réinitialisés lorsque le certificat ITLRecovery est régénéré sur l'éditeur ou l'un des abonnés. Une fois le certificat ITLRecovery régénéré, le fichier ITL ne se met à jour que lorsque le service TFTP est redémarré. Après la régénération du certificat ITLRecovery sur l'éditeur, redémarrez le service TFTP sur chaque noeud qui exécute le service TFTP dans le cluster afin de mettre à jour l'entrée ITLRecovery dans le fichier ITL avec le nouveau certificat. La dernière étape consiste à réinitialiser tous les périphériques à partir de **System > Enterprise Parameters** et à utiliser le bouton reset afin que tous les périphériques téléchargent le nouveau fichier ITL qui contient le nouveau certificat ITLRecovery.

Sauvegarder la récupération ITL

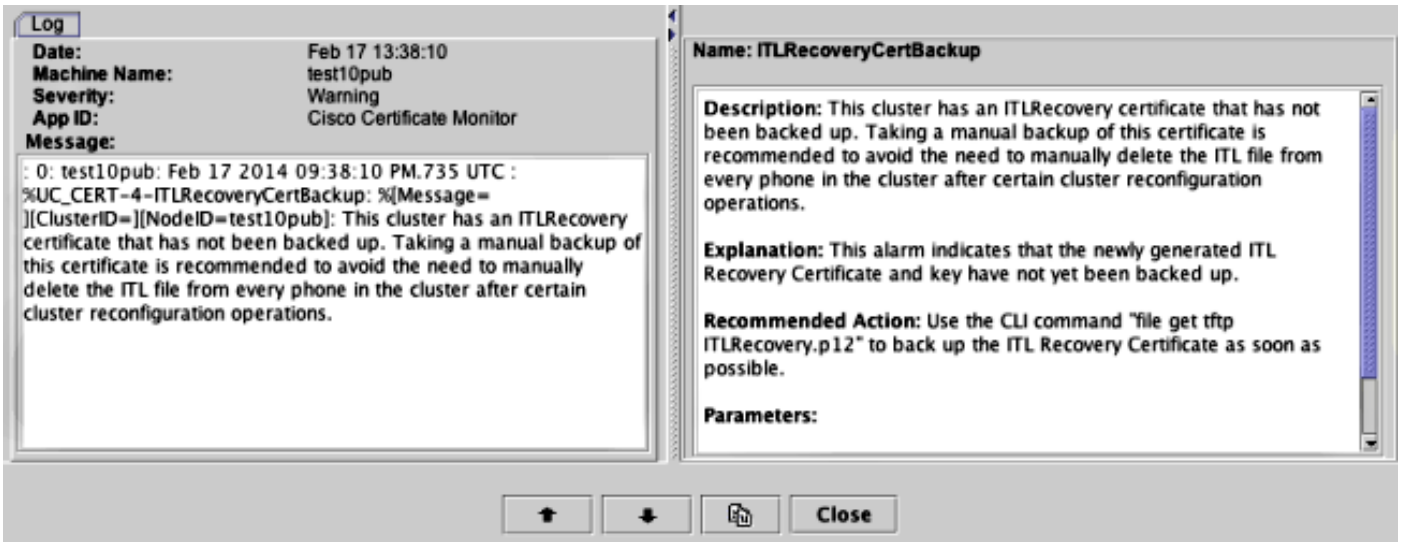
La clé de récupération ITL est requise pour récupérer les téléphones lorsqu'ils entrent dans un état non approuvé. De ce fait, de nouvelles alertes RTMT (Real-Time Monitoring Tool) sont générées quotidiennement jusqu'à ce que la clé de récupération ITL soit sauvegardée. Une sauvegarde DRS (Disaster Recovery System) ne suffit pas pour arrêter les alertes. Bien qu'une sauvegarde soit recommandée pour enregistrer la clé de récupération ITL, une sauvegarde manuelle du fichier de clé est également nécessaire.

Afin de sauvegarder la clé de récupération, connectez-vous à l'interface de ligne de commande de l'éditeur et entrez la commande **get tftp ITLRecovery.p12**. Un serveur SFTP est nécessaire pour enregistrer le fichier comme indiqué ici. Les noeuds d'abonné n'ont pas de fichier de récupération

ITL. Par conséquent, si vous émettez la commande **get tftp ITLRecovery.p12** sur un abonné, le **fichier** est **introuvable**.

```
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 effectuée à partir de l'interface de ligne de commande afin de sauvegarder le fichier ITLRecovery.p12, un avertissement est imprimé chaque jour dans CiscoSyslog (Observateur d'événements - Journal d'applications), comme indiqué ici. Un e-mail quotidien peut également être reçu jusqu'à ce que la sauvegarde manuelle soit effectuée si la notification par e-mail est activée à partir de la page d'administration du système d'exploitation, **Security > Certificate Monitor**.



Alors qu'une sauvegarde DRS contient ITLRecovery, il est recommandé de conserver le fichier ITLRecovery.p12 dans un emplacement sûr en cas de perte ou de corruption des fichiers de sauvegarde ou afin d'avoir la possibilité de réinitialiser le fichier ITL sans avoir besoin de restaurer à partir d'une sauvegarde. Si vous avez enregistré le fichier ITLRecovery.p12 de l'éditeur, il permet également à l'éditeur d'être reconstruit sans sauvegarde avec l'option de restauration DRS pour restaurer la base de données à partir d'un abonné et rétablir la confiance entre les téléphones et les serveurs CUCM en réinitialisant l'ITL avec l'option **utils itl reset remotekey**.

N'oubliez pas que si l'éditeur est reconstruit, le mot de passe de sécurité du cluster doit être identique à celui de l'éditeur à partir duquel le fichier ITLRecovery.p12 a été extrait, car le fichier

ITLRecovery.p12 est protégé par mot de passe avec un mot de passe basé sur le mot de passe de sécurité du cluster. Pour cette raison, si le mot de passe de sécurité du cluster est modifié, l'alerte RTMT qui indique que le fichier ITLRecovery.p12 n'a pas été sauvegardé est réinitialisée et se déclenche tous les jours jusqu'à ce que le nouveau fichier ITLRecovery.p12 soit enregistré avec la commande **get tftp ITLRecovery.p12**.

Vérification

La fonctionnalité de réinitialisation ITL en bloc ne fonctionne que si un ITL installé sur les téléphones contient l'entrée ITLRecovery. Afin de vérifier que le fichier ITL installé sur les téléphones contient l'entrée ITLRecovery, entrez la commande **show itl** à partir de l'interface de ligne de commande sur chacun des serveurs TFTP pour trouver la somme de contrôle du fichier ITL. La sortie de la commande **show itl** 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, car chaque serveur a son propre certificat **callmanager.pem** dans son fichier ITL. La somme de contrôle ITL de l'ITL installé sur le téléphone peut être trouvée si vous affichez l'ITL sur le téléphone lui-même sous **Paramètres > Configuration de sécurité > Liste de confiance**, à partir de la page Web du téléphone ou de l'alarme DeviceTLInfo signalée par les téléphones qui exécutent un micrologiciel plus récent.

La plupart des téléphones qui exécutent le microprogramme version 9.4(1) ou ultérieure signalent le hachage SHA1 de leur ITL à CUCM avec l'alarme DeviceTLInfo. Les informations envoyées par le téléphone peuvent être affichées dans l'Observateur d'événements - Journal d'applications de RTMT et comparées au hachage SHA1 du hachage ITL des serveurs TFTP que les téléphones utilisent afin de trouver tous les téléphones qui n'ont pas installé l'ITL actuel, qui contient l'entrée ITLRecovery.

Cavates

- CSCun18578 - La réinitialisation ITL de clé locale/de touche à distance échoue dans certains scénarios
- CSCun19112 - Erreur ITL reset remotekey dans le type d'authentification SFTP incorrect