Mejoras de Unified Communications Manager ITL en la versión 10.0(1)

Contenido

Introducción

Este documento describe una nueva función de Cisco Unified Communications Manager (CUCM) versión 10.0(1) que permite el restablecimiento masivo de los archivos de la lista de confianza de identidad (ITL) en los teléfonos IP de Cisco Unified. La función de restablecimiento masivo de ITL se utiliza cuando los teléfonos ya no confían en el firmante del archivo ITL y tampoco pueden autenticar el archivo ITL proporcionado localmente por el servicio TFTP o con el uso del Servicio de verificación de confianza (TVS).

Background

La capacidad de restablecer de forma masiva los archivos ITL evita la necesidad de realizar uno o varios de estos pasos para restablecer la confianza entre los teléfonos IP y los servidores CUCM.

- Restauración desde una copia de seguridad para cargar un archivo ITL antiguo en el que confían los teléfonos
- Cambie los teléfonos para utilizar un servidor TFTP diferente
- Elimine el archivo ITL del teléfono manualmente a través del menú de configuración
- Restablezca la configuración de fábrica del teléfono en la configuración del evento de modo que el acceso esté desactivado para borrar el ITL

Esta función no está diseñada para mover teléfonos entre clústeres; para esa tarea, utilice uno de los métodos descritos en Migración de Teléfonos IP entre Clústeres con Archivos CUCM 8 e ITL.

La operación de reinicio ITL se utiliza solamente para restablecer la confianza entre los teléfonos IP y el clúster CUCM cuando han perdido sus puntos de confianza.

Otra función relacionada con la seguridad disponible en la versión 10.0(1) de CUCM que no se incluye en este documento es la Lista de confianza de certificados sin Tokenless (CTL). El CTL sin Tokenless reemplaza los tokens de seguridad USB de hardware por un token de software utilizado para habilitar el cifrado en los servidores y terminales de CUCM. Para obtener información adicional, consulte el documento Seguridad del teléfono IP y CTL (Lista de confianza de certificados).

De forma predeterminada, se puede encontrar información adicional sobre los archivos ITL y la seguridad en el documento Communications Manager Security By Default y ITL Operation and Troubleshooting.

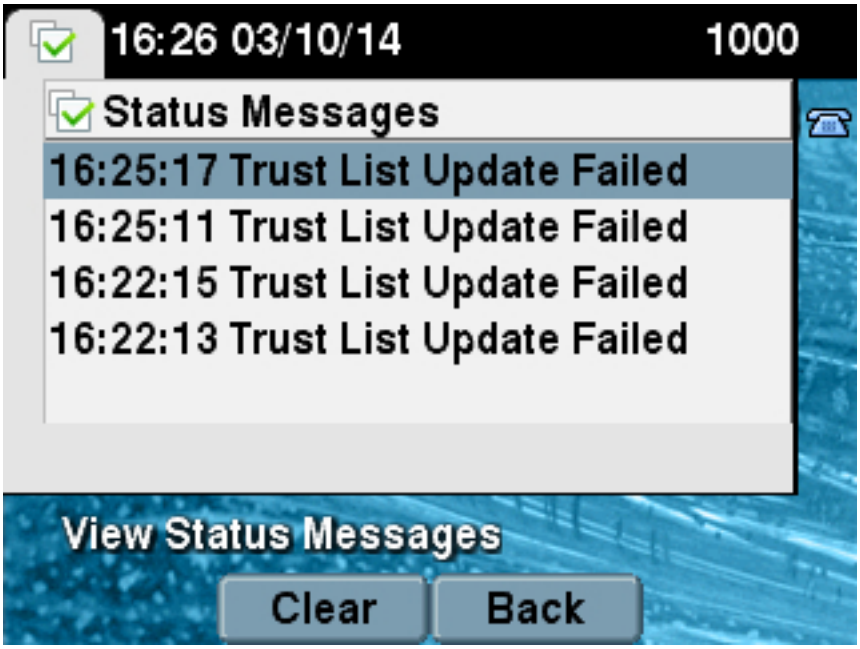
Indicios de problema

Cuando los teléfonos están en un estado **bloqueado** o **no confiable**, no aceptan el archivo ITL o la configuración TFTP proporcionada por el servicio TFTP. Cualquier cambio de configuración que se contenga en el archivo de configuración TFTP no se aplica al teléfono. Algunos ejemplos de configuración que se incluyen en el archivo de configuración TFTP son:

- Acceso a configuración
- Acceso web
- Acceso de Secure Shell (SSH)
- Analizador de puerto conmutado (SPAN) a puerto PC

Si se cambia alguno de estos parámetros para un teléfono en la página Administrador de CCM y, después de restablecer el teléfono, los cambios no surten efecto, es posible que el teléfono no confíe en el servidor TFTP. Otro síntoma común es cuando se accede al directorio corporativo u otros servicios telefónicos, se muestra el mensaje **Host Not Found**. Para verificar que el teléfono está en estado bloqueado o no confiable, verifique los mensajes de estado del teléfono del teléfono mismo o de la página web del teléfono para ver si aparece un mensaje **Trust List Update Failed**. El mensaje **ITL Update Failed** es un indicador de que el teléfono se encuentra en un estado bloqueado o no confiable porque no ha podido autenticar la lista de confianza con su ITL actual y no pudo autenticarlo con TVS.

El mensaje **Trust List Update Failed** se puede ver desde el propio teléfono si navega hasta **Settings > Status > Status Messages**:



El mensaje **Trust List Update Failed también se puede ver desde la página web del teléfono desde los Mensajes de Estado** como se muestra aquí:

Solución - Reinicio masivo de ITL

La versión 10.0(1) de CUCM utiliza una clave adicional que se puede utilizar para restablecer la confianza entre los teléfonos y los servidores CUCM. Esta nueva clave es la clave de recuperación de ITL. La clave ITL Recovery se crea durante la instalación o actualización. Esta clave de recuperación no cambia cuando se realizan cambios de nombre de host, cambios de DNS u otros cambios que pueden provocar problemas cuando los teléfonos alcanzan un estado en el que ya no confían en el firmante de sus archivos de configuración.

El nuevo comando CLI **utils itl reset** se puede utilizar para restablecer la confianza entre un teléfono o teléfonos y el servicio TFTP en CUCM cuando los teléfonos se encuentran en un estado donde se ve el mensaje **Trust List Update Failed**. El comando **utils itl reset**:

1. Toma el archivo ITL actual del nodo del editor, elimina la firma del archivo ITL y firma de nuevo el contenido del archivo ITL con la clave privada ITL Recovery.
2. Copia automáticamente el nuevo archivo ITL a los directorios TFTP en todos los nodos TFTP activos del clúster.
3. Reinicia automáticamente los servicios TFTP en cada nodo donde se ejecuta TFTP.

A continuación, el administrador debe restablecer todos los teléfonos. El reinicio hace que los

teléfonos soliciten el archivo ITL al arrancar desde el servidor TFTP y el archivo ITL que recibe el teléfono está firmado por la clave ITLRecrecovery en lugar de la clave **callmanager.pem** privada. Hay dos opciones para ejecutar un reinicio de ITL: **utils itl reset localkey** y **utils itl reset remotekey**. El comando ITL reset sólo se puede ejecutar desde el editor. Si ejecuta un reinicio de ITL desde un suscriptor, se obtiene el mensaje **This is not a Publisher Node** . Los ejemplos de cada comando se detallan en las siguientes secciones.

Recuperación de ITLR con la clave de recuperación local

La opción localkey utiliza la clave privada ITL Recovery contenida en el archivo ITLRecrecovery.p12 presente en el disco duro del editor como el nuevo firmante del archivo 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
```

Recuperación de ITLR con la clave de recuperación remota

La opción remotekey permite especificar el servidor SFTP externo desde el que se ha guardado el archivo ITLRecrecovery.p12.

```
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
```

Nota: Si se realiza un reinicio ITL con la opción remotekey, la clave local (en el archivo de disco) del editor se reemplaza por la clave remota.

Verifique el firmante actual con el comando "show itl"

Si ve el archivo ITL con el comando **show itl** antes de ejecutar un comando de reinicio ITL, muestra que ITL contiene una entrada **ITLRECOVERY_*<nombre_host>*** . Cada archivo ITL que se suministra por cualquier servidor TFTP en el clúster contiene esta entrada de recuperación ITL del editor. La salida del comando **show itl** se toma del editor en este ejemplo. El token utilizado para firmar el ITL está en negrita:

```
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.
```

Verifique que ITLRecrecovery Key se use

Si ve el archivo ITL con el comando **show itl** después de realizar un reinicio ITL, muestra que la entrada ITLRecrecovery ha firmado el ITL como se muestra aquí. ITLRecrecovery sigue siendo el firmante del ITL hasta que se reinicie el TFTP, momento en el que se utiliza el **callmanager.pem** o el certificado TFTP para firmar el ITL de nuevo.

```
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.
```

Mejoras para reducir la posibilidad de que los teléfonos pierdan confianza

Además de la capacidad de reinicio de ITL, CUCM versión 10.0(1) incluye funciones de administrador que ayudan a evitar que los teléfonos entren en un estado no confiable. Los dos puntos de confianza que tiene el teléfono son el certificado TVS (**TVS.pem**) y el certificado TFTP (**callmanager.pem**). En el entorno más sencillo con sólo un servidor CUCM, si un administrador regenera el certificado **callmanager.pem** y el certificado **TVS.pem** uno tras otro, el teléfono se restablece y, al iniciar, muestra el mensaje **Trust List Update Failed**. Incluso con un reinicio automático del dispositivo enviado desde CUCM al teléfono debido a un certificado contenido en el ITL que se regenera, el teléfono puede ingresar un estado donde no confía en CUCM.

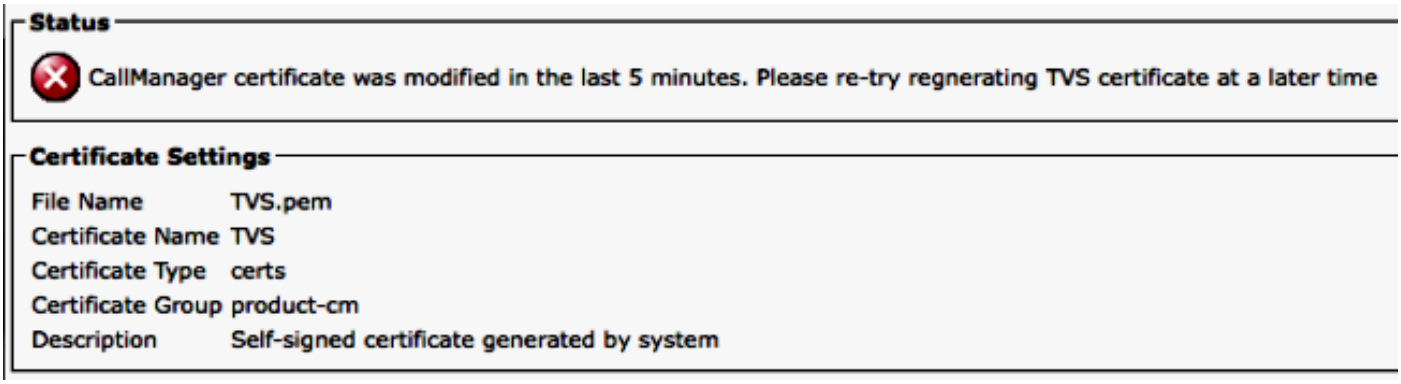
Para ayudar a evitar la situación en la que se regeneran varios certificados al mismo tiempo (por lo general, cambio de nombre de host o modificaciones de nombre de dominio DNS), CUCM ahora tiene un temporizador de espera. Cuando se regenera un certificado, CUCM impide que el administrador vuelva a generar otro certificado en el mismo nodo en un plazo de cinco minutos a partir de la regeneración del certificado anterior. Este proceso hace que los teléfonos se restablezcan al regenerar el primer certificado, y se deben realizar copias de seguridad y registrar antes de regenerar el siguiente certificado.

Independientemente del certificado que se genere primero, el teléfono tiene su método secundario para autenticar archivos. Puede encontrar detalles adicionales sobre este proceso en Communications Manager Security By Default y ITL Operation and Troubleshooting.

Este resultado muestra una situación en la que CUCM impide al administrador regenerar otro certificado dentro de los cinco minutos siguientes a la regeneración de un certificado anterior, tal como se ve desde la 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
```

Se puede ver el mismo mensaje desde la página de administración del sistema operativo (OS), como se muestra aquí:



La clave de recuperación ITL del editor es la única en uso por todo el clúster, aunque cada nodo tiene su propio certificado ITLRecrecovery emitido al Common Name (CN) de **ITLRecrecovery_*<node name>***. La clave ITLRecrecovery del editor es la única que se utiliza en los archivos ITL para todo el clúster como se ve en el comando **show itl**. Por eso la única **entrada ITLRecrecovery_*<hostname>*** vista en un archivo ITL contiene el nombre de host del editor.

Si se cambia el nombre de host del editor, la entrada ITLRecrecovery en el DIT sigue mostrando el nombre de host antiguo del editor. Esto se hace intencionalmente porque el archivo ITLRecrecovery nunca debería cambiar para asegurarse de que los teléfonos siempre confíen en la recuperación del ITL.

Esto se aplica cuando también se cambian los nombres de dominio; el nombre de dominio original se ve en la entrada ITLRecrecovery para asegurarse de que la clave de recuperación no cambie. La única vez que el certificado ITLRecrecovery debe cambiar es cuando caduque debido a la validez de cinco años y debe regenerarse.

Los pares de claves de recuperación de ITL se pueden regenerar con la CLI o la página de administración del sistema operativo. Los teléfonos IP no se restablecen cuando el certificado ITLRecrecovery se regenera en el editor o en cualquiera de los suscriptores. Una vez que se ha regenerado el certificado ITLRecrecovery, el archivo ITL no se actualiza hasta que se reinicie el servicio TFTP. Después de la regeneración del certificado de recuperación ITLR en el editor, reinicie el servicio TFTP en cada nodo que ejecute el servicio TFTP en el clúster para actualizar la entrada ITLRecrecovery en el archivo ITL con el nuevo certificado. El último paso es restablecer todos los dispositivos desde **System > Enterprise Parameters** y utilizar el botón reset para hacer que todos los dispositivos descarguen el nuevo archivo ITL que contiene el nuevo certificado ITLRecrecovery.

Copia de seguridad de la recuperación de ITL

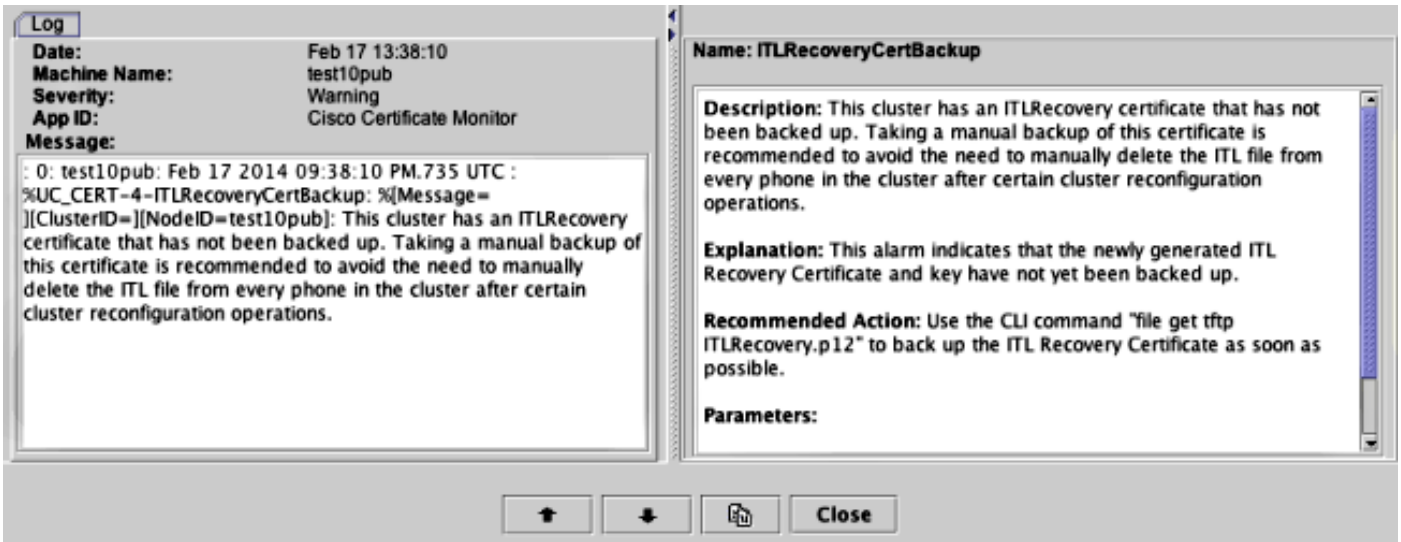
Se requiere la clave de recuperación de ITL para recuperar los teléfonos cuando ingresan a un estado no confiable. Debido a esto, se generan nuevas alertas de la Herramienta de supervisión en tiempo real (RTMT) diariamente hasta que se realiza una copia de seguridad de la clave de recuperación de ITL. Una copia de seguridad del sistema de recuperación ante desastres (DRS) no es suficiente para detener las alertas. Aunque se recomienda realizar una copia de seguridad para guardar la clave ITL Recovery, también se necesita una copia de seguridad manual del archivo de clave.

Para realizar una copia de seguridad de la clave de recuperación, inicie sesión en la CLI del editor e ingrese el comando **file get tftp ITLRecrecovery.p12**. Se necesita un servidor SFTP para guardar el archivo en como se muestra aquí. Los nodos del suscriptor no tienen un archivo de

recuperación ITL, por lo que si ejecuta el comando **file get tftp ITLRecrecovery.p12** en un suscriptor, se produce un **archivo no encontrado**.

```
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
```

Hasta que se realice la copia de seguridad manual desde la CLI para realizar una copia de seguridad del archivo ITLRecrecovery.p12, todos los días se imprime una advertencia en CiscoSyslog (Event Viewer - Application Log) como se muestra aquí. También se puede recibir un correo electrónico diario hasta que se realice la copia de seguridad manual si se habilita la notificación por correo electrónico desde la página de administración del sistema operativo, **Seguridad > Monitor de certificado**.



Si bien una copia de seguridad de DRS contiene ITLRecrecovery, se recomienda almacenar el archivo ITLRecrecovery.p12 en una ubicación segura en caso de que los archivos de copia de seguridad se pierdan o estén dañados o para tener la opción de restablecer el archivo ITL sin necesidad de restaurar desde una copia de seguridad. Si tiene el archivo ITLRecrecovery.p12 del editor guardado, también permite que el editor se reconstruya sin una copia de seguridad con la opción de restauración DRS para restaurar la base de datos de un suscriptor y restablecer la confianza entre los teléfonos y los servidores CUCM restableciendo el ITL con la opción utils itl reset remote.

Recuerde que si se reconstruye el editor, la contraseña de seguridad del clúster debe ser la

misma que la del editor del que se tomó el archivo ITLRecrecovery.p12 porque el archivo ITLRecrecovery.p12 está protegido mediante contraseña con una contraseña basada en la contraseña de seguridad del clúster. Por esta razón, si se cambia la contraseña de seguridad del clúster, se restablece la alerta RTMT que indica que el archivo ITLRecrecovery.p12 no se ha copiado y se activa diariamente hasta que se guarde el nuevo archivo ITLRecrecovery.p12 con el comando **file get tftp ITLRecrecovery.p12**.

Verificación

La función de reinicio masivo de ITL sólo funciona si los teléfonos tienen un ITL instalado que contiene la entrada ITLRecrecovery. Para verificar que el archivo ITL instalado en los teléfonos contiene la entrada ITLRecrecovery, ingrese el comando **show itl** de la CLI en cada uno de los servidores TFTP para encontrar la suma de comprobación del archivo ITL. El resultado del comando **show itl** muestra la suma de comprobación:

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

La suma de comprobación es diferente en cada servidor TFTP porque cada servidor tiene su propio certificado **callmanager.pem** en su archivo ITL. La suma de comprobación ITL del ITL instalado en el teléfono se puede encontrar si ve el ITL en el teléfono mismo bajo **Configuración > Configuración de seguridad > Lista de confianza**, desde la página web del teléfono, o desde la alarma DeviceTLInfo informada por teléfonos que ejecutan firmware más reciente.

La mayoría de los teléfonos que ejecutan firmware versión 9.4(1) o posterior informan del hash SHA1 de su ITL a CUCM con la alarma DeviceTLInfo. La información enviada por el teléfono se puede ver en el Visor de eventos - Registro de aplicaciones desde RTMT y comparada con el hash SHA1 del hash ITL de los servidores TFTP que los teléfonos utilizan para encontrar cualquier teléfono que no tenga instalado el ITL actual, que contiene la entrada ITLRecrecovery.

Advertencias

- CSCun18578 - El reinicio de ITL de la clave local/remota falla en algunos escenarios
- CSCun19112 - Error de reinicio ITL de la clave remota en el tipo de autenticación SFTP incorrecta