Mejoras ITL del administrador de las Comunicaciones unificadas en la versión 10.0(1)

Contenido

Introducción

Este documento describe una nueva función en la versión 10.0(1) del administrador de las Comunicaciones unificadas de Cisco (CUCM) que habilita la restauración a granel de los archivos de la lista de la confianza de la identidad (ITL) en Cisco unificó los Teléfonos IP. Se utiliza la característica de la restauración ITL del bulto cuando los teléfonos confían en no más al firmante del archivo ITL y también no pueden autenticar el archivo ITL proporcionado por servicio TFTP localmente o el uso del servicio de la verificación de la confianza (TV).

Antecedente

La capacidad de abultar los archivos ITL de la restauración previene la necesidad de realizar uno o muchos de estos pasos para restablecer la confianza entre los Teléfonos IP y los servidores CUCM.

- Restore de un de reserva para cargar un viejo archivo ITL que los teléfonos confían en
- Cambie los teléfonos para utilizar a un diverso servidor TFTP
- Borre el archivo ITL del teléfono manualmente a través del menú de Configuración
- La fábrica reajustó el teléfono en las configuraciones de evento para inhabilitar el acceso para borrar la ITL

Esta característica no se piensa para mover los teléfonos entre los clusteres; para esa tarea, utilice uno de los métodos descritos en los Teléfonos IP de la migración entre los clusteres con los archivos CUCM 8 e ITL. La operación de la restauración ITL se utiliza para restablecer solamente

la confianza entre los Teléfonos IP y el cluster CUCM cuando han perdido sus puntas de la confianza.

Otra característica relacionada con la seguridad disponible en la versión 10.0(1) CUCM que no se cubre en este documento es la lista de la confianza de Tokenless Certficate (CTL). El Tokenless CTL substituye los tokenes de seguridad del hardware USB por para un Enable Encryption usado ficha de software en los servidores y los puntos finales CUCM. Para la información adicional, refiera a la Seguridad del teléfono del IP y al documento CTL (Certificate Trust List (Lista de confianza del certificado)).

La información adicional en los archivos y la Seguridad ITL por abandono se puede encontrar en la Seguridad del administrador de comunicaciones por abandono y operación y documento de Troubleshooting ITL.

Indicios de problema

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

- Acceso de las configuraciones
- Acceso Web
- Acceso del Secure Shell (SSH)
- Switched Port Analyzer (SPAN) al puerto de PC

Si ninguno de estos configuraciones se cambian para un teléfono en la página de administración de CCM y, después de que se reajuste el teléfono, los cambios no tome el efecto, el teléfono no pudo confiar en al servidor TFTP. Otro síntoma común es cuando usted accede Corporate Directory (Directorio corporativo) u otros servicios telefónicos, las visualizaciones **no encontradas del host del** mensaje. Para verificar que el teléfono esté en un bloqueado o estado no confiable, marque los mensajes de estado del teléfono sí mismo del teléfono o el Web page del teléfono para ver si las visualizaciones de la **confianza de la lista de un mensaje fallido de la actualización**. **El mensaje fallido de la actualización ITL** es un indicador que el teléfono está en un bloqueado o estado no confiable porque no ha podido autenticar la lista de la confianza con su ITL actual y no ha podido autenticarla con los TV.

El mensaje fallido de la actualización de la lista de la confianza se puede considerar del teléfono sí mismo si usted navega a las **configuraciones > al estatus > a los mensajes de estado**:

El mensaje fallido de la actualización de la lista de la confianza se puede también considerar de la página web del teléfono de los **mensajes de estado** como se muestra aquí:

Solución - Restauración a granel ITL

La versión 10.0(1) CUCM utiliza una clave adicional que se pueda utilizar para restablecer la confianza entre los teléfonos y los servidores CUCM. Esta nueva clave es la clave de la recuperación ITL. La clave de la recuperación ITL se crea durante el instalar o la actualización. Esta clave de la recuperación no cambia cuando el nombre de host cambia, DNS cambia, o se realizan otros cambios que pudieron llevar a los problemas adonde los teléfonos consiguen en un

estado donde confían en no más al firmante de sus archivos de configuración.

El nuevo comando CLI de la **restauración ITL del utils** puede ser utilizado para restablecer la confianza entre un teléfono o los teléfonos y servicio TFTP encendido el CUCM cuando los teléfonos son en un estado donde se considera el **mensaje fallido de la actualización de la lista de la confianza**. **El comando reset ITL del utils**:

1. Toma el archivo actual ITL del nodo del editor, elimina la firma del archivo ITL, y firma el contenido del archivo ITL otra vez con la clave privada de la recuperación ITL.
2. Copia automáticamente el nuevo archivo ITL a los directorios TFTP en todos los Nodos activos TFTP en el cluster.
3. Recomienza automáticamente los servicios TFTP en cada nodo adonde el TFTP se ejecuta.

El administrador debe entonces reajustar todos los teléfonos. La restauración hace los teléfonos pedir el archivo ITL sobre el inicio para arriba del servidor TFTP y el archivo ITL que el teléfono recibe es firmado por la clave de ITLRecovery en vez de la **clave privada callmanager.pem**. Hay dos opciones para funcionar con una ITL reajustada: **localkey de la restauración del** utilsitl **y remotekey de la restauración del** utilsitl**.** El comando reset ITL puede ser funcionado con solamente del editor. Si usted publica una ITL reajustada de un suscriptor, da lugar al Thisis **no un mensaje del nodo de Publisher**. Los ejemplos de cada comando se detallan en las siguientes secciones.

ITLRecovery con la clave local de la recuperación

La opción del localkey utiliza la clave privada de la recuperación ITL contenida en el archivo ITLRecovery.p12 presente en la unidad de disco duro de Publisher 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
```

ITLRecovery con la clave remota de la recuperación

La opción del remotekey permite al servidor SFTP externo de quien el archivo ITLRecovery.p12 se ha guardado para ser especificado.

```
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 una restauración ITL se hace con la opción del remotekey, el localkey (en el archivo del disco) en el editor se substituye por el remotekey.

Verifique al firmante actual con “el comando ITL de la demostración”

Si usted ve el archivo ITL con el comando **ITL de la demostración** antes de que usted publique un comando reset ITL, muestra que la ITL contiene una entrada del *<publisher_hostname>* **ITLRECOVERY_**. Cada archivo ITL que es servido por cualquier servidor TFTP en el cluster contiene esta entrada de la recuperación ITL del editor. La salida del comando **ITL de la demostración** se toma del editor en este ejemplo. El token usado para firmar la ITL está en intrépido:

```
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 la clave de ITLRecovery esté utilizada

Si usted ve el archivo ITL con el comando **ITL de la demostración** después de que usted realice una restauración ITL, muestra que la entrada de ITLRecovery ha firmado la ITL como se muestra

aquí. El ITLRecovery sigue siendo el firmante de la ITL hasta que se recomience el TFTP, en cuya hora el **callmanager.pem o el** certificado TFTP se utiliza para firmar la ITL otra vez.

```
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 disminuir la posibilidad de los teléfonos que pierden la confianza

Además de la capacidad de la restauración ITL, la versión 10.0(1) CUCM incluye las características del administrador que ayudan a evitar que los teléfonos ingresen estado no confiable. La confianza dos señala el teléfono tiene es el certificado TV (**TVS.pem) y el** certificado TFTP (callmanager.pem**). En el** entorno más simple con solamente un servidor CUCM, si un administrador regenera el callmanager.pemcertificate y el certificado uno TVS.pem justo después de otro, las restauraciones del teléfono y sobre el bootup visualizan el **mensaje fallido de la actualización de la** lista de la confianza**. Incluso** con una restauración del dispositivo automático enviada de CUCM al teléfono debido a un certificado contenido en la ITL se regenera que, el teléfono puede ingresar un estado donde no confía en CUCM.

Para ayudar a prevenir el escenario donde los certificados múltiples se regeneran al mismo tiempo (típicamente cambio del nombre de host o las modificaciones del Domain Name DNS), CUCM ahora tiene un temporizador del control. Cuando se regenera un certificado, CUCM evita que el administrador regenere otro certificado en el mismo nodo en el plazo de cinco minutos de la regeneración anterior del certificado. Este proceso hace los teléfonos ser reajustado sobre la regeneración del primer certificado, y deben ser salvaguardia y registrado antes de que se regenere el certificado siguiente.

Sin importar qué certificado se genera primero, el teléfono tiene su método secundario para autenticar los archivos. Los detalles adicionales sobre este proceso pueden ser encontrados en la Seguridad del administrador de comunicaciones por abandono y operación y troubleshooting ITL.

Esta salida muestra a situación donde CUCM evita que el administrador regenere otro certificado en el plazo de cinco minutos de una regeneración anterior del certificado según lo visto del 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
```

El mismo mensaje se puede considerar de la página de administración del operating system (OS) como se muestra aquí:

La clave de la recuperación ITL del editor es la única funcionando por el cluster entero, aunque cada nodo tiene su propio certificado de ITLRecovery publicado al Common Name (CN) de **ITLRecovery_ *<node name>***. La clave de ITLRecovery del editor es la única usada en los archivos ITL para el cluster entero según lo considerado del comando **ITL de la demostración**. Esta es la razón por la cual la única entrada del ***<hostname> de*** **ITLRecovery_** considerada en un archivo ITL contiene el nombre de host del editor.

Si el nombre de host del editor se cambia, la entrada de ITLRecovery en la ITL continúa mostrando el nombre de host viejo del editor. Esto se hace intencionalmente porque el archivo de ITLRecovery debe nunca cambiar para asegurar a la confianza de los teléfonos siempre la recuperación ITL.

Esto solicita cuando los Domain Name se cambian también; el nombre de dominio original se considera en la entrada de ITLRecovery para asegurarse de que la clave de la recuperación no cambia. La única vez que el certificado de ITLRecovery debe cambiar es cuando expira debido a la validez de cinco años y debe ser regenerado.

Los keypairs de la recuperación ITL se pueden regenerar con el CLI o la página de administración OS. Los Teléfonos IP no se reajustan cuando el certificado de ITLRecovery se regenera en el editor o los suscriptores uces de los. Una vez que se ha regenerado el certificado de ITLRecovery, el archivo ITL no se pone al día hasta que servicio TFTP se recomience. Después de la regeneración del certificado de ITLRecovery en el editor, recomience servicio TFTP encendido el cada nodo que ejecuta servicio TFTP adentro el cluster para poner al día la entrada de ITLRecovery en el archivo ITL con el nuevo certificado. El último paso es reajustar todos los dispositivos del **System (Sistema) > Enterprise Parameters (Parámetros Enterprise)** y utilizar el botón reset para hacer toda la descarga de los dispositivos el nuevo archivo ITL que contiene el nuevo certificado de ITLRecovery.

Sostenga la recuperación ITL

La clave de la recuperación ITL se requiere para recuperar los teléfonos cuando ingresan estado no confiable. Debido a esto, las nuevas alertas de la herramienta del monitoreo en tiempo real (RTMT) se generan diariamente hasta que se sostenga la clave de la recuperación ITL. Un respaldo del sistema de la Recuperación tras desastres (DR) no es suficiente parar las alertas. Aunque un respaldo se recomiende para salvar la clave de la recuperación ITL, un respaldo manual del archivo clave se necesita también.

Para sostener la clave de la recuperación, el login al CLI del editor y ingresar el **archivo consigue el** comando del **tftp ITLRecovery.p12**. Un servidor SFTP es necesario para salvar el archivo a como se muestra aquí. Los Nodos del suscriptor no tienen un archivo de recuperación ITL, así que si usted publica el **archivo consiguen el** comando de **tftp ITLRecovery.p12** en un suscriptor, él dan lugar al **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 el respaldo manual se realice del CLI para sostener el archivo ITLRecovery.p12, una advertencia se imprime en el CiscoSyslog (registro de la aplicación del visor de eventos) cada día como se muestra aquí. Un correo electrónico diario pudo también ser recibido hasta que se realice el respaldo manual si la notificación por correo electrónico se habilita de la página de administración OS, **Seguridad > monitor del certificado**.

Mientras que un respaldo DR contiene el ITLRecovery, se recomienda todavía para salvar el archivo ITLRecovery.p12 en una ubicación segura en caso de que se pierdan o se corrompan los archivos de backup o para tener la opción para reajustar el archivo ITL sin la necesidad de restablecer de un respaldo. Si usted tiene el archivo ITLRecovery.p12 del editor guardado, también permite que al editor reconstruya sin un respaldo con el uso la opción del restore DR de restablecer la base de datos de un susbcriber y de restablecer la confianza entre los teléfonos y los servidores CUCM reajustando la ITL con la opción del **remotekey de la restauración ITL del utils**.

Recuerde que si reconstruyen al editor, la contraseña de seguridad del cluster debe ser lo mismo que el editor del donde el archivo ITLRecovery.p12 fue tomado porque el archivo ITLRecovery.p12 es protegidas por contraseña con una contraseña basada apagado de la contraseña de seguridad del cluster. Por este motivo, si se cambia la contraseña de seguridad del cluster, el RTMT alerta que indica que el archivo ITLRecovery.p12 no se ha sostenido se reajusta y acciona el diario hasta que el nuevo archivo ITLRecovery.p12 se guarde con el **archivo consiga el** comando de **tftp ITLRecovery.p12**.

Verificación

La característica de la restauración ITL del bulto trabaja solamente si los teléfonos tienen una ITL instalada que contenga la entrada de ITLRecovery. Para verificar que el archivo ITL instalado en los teléfonos contenga la entrada de ITLRecovery, ingrese el comando **ITL de la demostración del** CLI en cada uno de los servidores TFTP de encontrar la suma de comprobación del archivo ITL. La salida del comando **ITL de la demostración** visualiza 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 de la ITL instalada en el teléfono puede ser encontrada si usted ve la ITL en el teléfono sí mismo conforme a la **configuración del > Security (Seguridad) de las** configuraciones **> a la lista de la confianza, de la** página web del teléfono, o de la alarma de DeviceTLInfo señalada por los teléfonos que funcionan con un más nuevo firmware.

La mayoría de los teléfonos que funcionan con la versión de firmware 9.4(1) o el informe posterior el hash SHA1 de su ITL a CUCM con la alarma de DeviceTLInfo. La información enviada por el teléfono se puede ver en el registro de la aplicación del visor de eventos de RTMT y comparar al hash SHA1 del hash ITL de los servidores TFTP el uso de los teléfonos para encontrar cualquier teléfono que no tenga la ITL actual instalada, que contiene la entrada de ITLRecovery.

Advertencias

- CSCun18578 - La restauración localkey/remotekey ITL falla en ciertos escenarios
- CSCun19112 - Error del remotekey de la restauración ITL en el tipo de la autentificación que resultó mal SFTP