Realces ITL do gerente das comunicações unificadas na versão 10.0(1)

Índice

Introdução

Este documento descreve uns novos recursos na versão 10.0(1) do gerente das comunicações unificadas de Cisco (CUCM) que permite a restauração maioria de arquivos da lista da confiança da identidade (ITL) em Cisco unificou Telefones IP. A característica da restauração ITL do volume é usada quando os telefones já não confiam o signatário do arquivo ITL e igualmente não podem autenticar o arquivo ITL fornecido pelo serviço TFTP localmente ou com o uso do serviço da verificação da confiança (TV).

Background

A capacidade para aumentar arquivos ITL da restauração impede a necessidade de executar uma ou muitas destas etapas para restabelecer a confiança entre Telefones IP e os server CUCM.

- Restauração de um alternativo a fim transferir arquivos pela rede um arquivo velho ITL que os telefones confiem
- Mude os telefones a fim usar um servidor TFTP diferente
- Suprima do arquivo ITL do telefone manualmente através do menu de configurações
- A fábrica restaurou o telefone nas configurações de evento de modo que o acesso fosse desabilitado a fim apagar a ITL

Esta característica não é pretendida mover telefones entre conjuntos; para essa tarefa, use um dos métodos descritos em [Telefones IP da migração entre conjuntos com arquivos CUCM 8 e](#)

ITL. A operação da restauração ITL está usada para restabelecer somente a confiança entre Telefones IP e o conjunto CUCM quando perderam seus pontos da confiança.

Uma outra característica relacionado à segurança disponível na versão 10.0(1) CUCM que não é coberta neste documento é a lista da confiança de Tokenless Certficate (CTL). O Tokenless CTL substitui os tokens de segurança do hardware USB com um Enable Encryption usado token de software nos server e em valores-limite CUCM. Para a informação adicional, refira a Segurança do telefone IP e o documento CTL (certificate trust list).

A informação adicional nos arquivos e a Segurança ITL à revelia pode ser encontrada na Segurança do Gerenciador de Comunicações à revelia e operação e documento de Troubleshooting ITL.

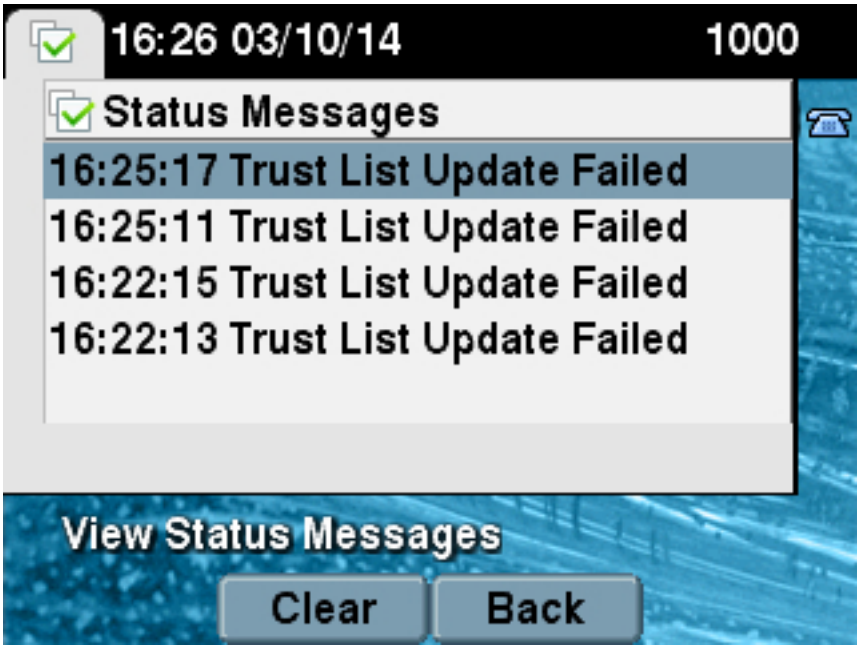
Sintomas do problema

Quando os telefones estão em um **fechado** ou em um **estado não-confiável**, não aceitam o arquivo ou a configuração de TFTP ITL fornecido pelo serviço TFTP. Nenhuma alteração de configuração que for contida no arquivo de configuração de TFTP não é aplicada ao telefone. Alguns exemplos dos ajustes que são contidos no arquivo de configuração de TFTP são:

- Acesso dos ajustes
- Acesso à Web
- Acesso do Shell Seguro (ssh)
- Switched Port Analyzer (SPAN) à porta de PC

Se qualquens um ajustes estão mudados para um telefone na página de admin CCM e, depois que o telefone está restaurado, as mudanças não tome o efeito, o telefone não pôde confiar o servidor TFTP. Um outro sintoma comum é quando você alcança o diretório corporativo ou outros serviços de telefone, os indicadores **não encontrados do host da** mensagem. A fim verificar que o telefone está em um fechado ou em um estado não-confiável, verifique os mensagens de status do telefone próprios do telefone ou o página da web do telefone a fim ver se indicadores de **falha de mensagem da atualização da lista da confiança**. **A falha de mensagem da atualização ITL** é um indicador que o telefone está em um fechado ou em um estado não-confiável porque não autenticou a lista da confiança com sua ITL atual e não a autenticou com TV.

A falha de mensagem da atualização da lista da confiança pode ser considerada do telefone próprio se você navega aos **ajustes > ao estado > aos mensagens de status**:



A falha de mensagem da atualização da lista da confiança pode igualmente ser considerada do página da web do telefone dos **mensagens de status** como mostrado aqui:

Solução - Restauração maioria ITL

A versão 10.0(1) CUCM usa uma chave adicional que possa ser usada a fim restabelecer a confiança entre telefones e os server CUCM. Esta chave nova é a chave da recuperação ITL. A chave da recuperação ITL é criada durante a instalação ou a elevação. Esta chave da recuperação não muda quando o hostname muda, DNS muda, ou outras mudanças são executadas que puderam conduzir aos problemas aonde os telefones obtêm em um estado onde já não confiem o signatário de seus arquivos de configuração.

O comando CLI novo da **restauração ITL dos utils** pode ser usado a fim restabelecer a confiança entre um telefone ou uns telefones e o serviço TFTP em CUCM quando os telefones são em um estado onde a **falha de mensagem da atualização da lista da confiança** esteja considerada. **O comando reset ITL dos utils**:

1. Toma o arquivo atual ITL do nó do editor, descasca a assinatura do arquivo ITL, e assina os índices do arquivo ITL outra vez com a chave privada da recuperação ITL.
2. Copia automaticamente o arquivo novo ITL aos diretórios de TFTP em todos os Nós ativos TFTP no conjunto.
3. Reinicia automaticamente os serviços TFTP em cada nó aonde o TFTP é executado.

O administrador deve então restaurar todos os telefones. A restauração faz com que os telefones peçam o arquivo ITL em cima da bota acima do servidor TFTP e o arquivo que ITL o telefone recebe é assinado pela chave de ITLRecovery em vez da **chave privada callmanager.pem**. Há duas opções para executar uma ITL restaurada: **localkey da restauração do** utilsitl **e remotekey da restauração do** utilsitl**.** O comando reset ITL pode somente ser executado do editor. Se você emite uma ITL restaurada de um subscritor, conduz ao Thisis **não uma mensagem do nó do editor**. Os exemplos de cada comando são detalhados nas próximas seções.

ITLRecovery com a chave local da recuperação

A opção do localkey usa a chave privada da recuperação ITL contida no arquivo ITLRecovery.p12 atual no disco rígido do editor como o signatário novo do arquivo 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 com a chave remota da recuperação

A opção do remotekey permite o servidor SFTP externo de que o arquivo ITLRecovery.p12 salvar 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: Se uma restauração ITL é feita com a opção do remotekey, o localkey (no arquivo de disco) no editor está substituído com o remotekey.

Verifique o signatário atual com da “o comando ITL mostra”

Se você vê o arquivo ITL com o comando **ITL da mostra** antes que você emita um comando reset ITL, mostra que a ITL contém uma entrada do ***<publisher_hostname>*** **ITLRECOVERY_**. Cada arquivo ITL que é servido por todo o servidor TFTP no conjunto contém esta entrada da recuperação ITL do editor. A saída do comando **ITL da mostra** é tomada do editor neste exemplo. O token usado a fim assinar a ITL está em corajoso:

```
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 a chave de ITLRecovery está usada

Se você vê o arquivo ITL com o comando **ITL da mostra** depois que você executa uma restauração ITL, mostra que a entrada de ITLRecovery assinou a ITL como mostrado aqui. O ITLRecovery permanece o signatário da ITL até que o TFTP esteja reiniciado, quando o **callmanager.pem ou o** certificado TFTP estão usados a fim assinar outra vez a 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.
```

Realces para diminuir a possibilidade de telefones que perdem a confiança

Além do que a capacidade da restauração ITL, a versão 10.0(1) CUCM inclui as características do administrador que ajudam a impedir que os telefones entrem em um estado não-confiável. A confiança dois aponta o telefone tem é o certificado TV (**TVS.pem) e o** certificado TFTP (callmanager.pem**).** No ambiente o mais simples com o somente um server CUCM, se um administrador regenera o callmanager.pemcertificate e o certificado um TVS.pem mesmo após outro, as restaurações do telefone e em cima da inicialização indicam a **falha de mensagem da atualização da** lista da confiança**. Mesmo** com uma restauração do dispositivo automático enviada de CUCM ao telefone devido a um certificado contido na ITL que é regenerada, o telefone pode incorporar um estado onde não confie CUCM.

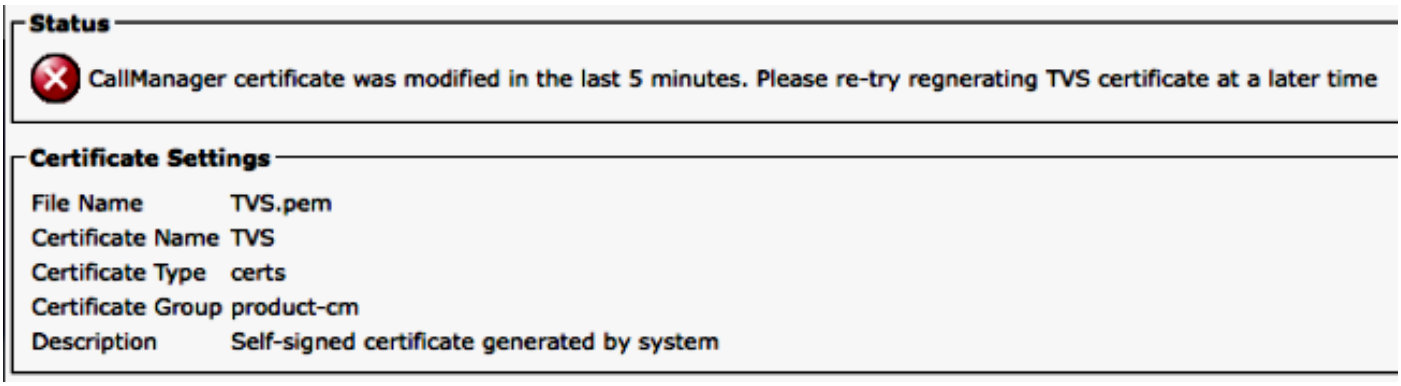
A fim ajudar a impedir a encenação onde os certificados múltiplos são regenerados ao mesmo tempo (tipicamente mudança do hostname ou de Domain Name DNS alterações), CUCM tem agora um temporizador da posse. Quando um certificado é regenerado, CUCM impede que o administrador regenere um outro certificado no mesmo nó dentro de cinco minutos da regeneração precedente do certificado. Este processo faz com que os telefones sejam restaurados em cima de regenerar o primeiro certificado, e devem ser apoio e registrado antes que o certificado seguinte esteja regenerado.

Apesar do que certificado é gerado primeiramente, o telefone tem seu método secundário para autenticar arquivos. Os detalhes adicionais sobre este processo podem ser encontrados na Segurança do Gerenciador de Comunicações à revelia e operação e Troubleshooting ITL.

Esta saída mostra a uma situação onde CUCM impede que o administrador regenere um outro certificado dentro de cinco minutos de uma regeneração precedente do certificado como vistos do 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
```

A mesma mensagem pode ser considerada da página de administração do operating system (OS) como mostrado aqui:



A chave da recuperação ITL do editor é única no uso pelo conjunto inteiro, mesmo que cada nó tenha seu próprio certificado de ITLRecovery emitido ao Common Name (CN) do *name> do <node de* ITLRecovery_. A chave de ITLRecovery do editor é única usada nos arquivos ITL para o conjunto inteiro como considerado do comando **ITL da mostra**. Eis porque a única entrada do *<hostname> de* ITLRecovery_ considerada em um arquivo ITL contém o hostname do editor.

Se o hostname do editor é mudado, a entrada de ITLRecovery na ITL continua a mostrar o hostname velho do editor. Isto é feito intencionalmente porque o arquivo de ITLRecovery deve nunca mudar para assegurar sempre à confiança dos telefones a recuperação ITL.

Isto aplica-se para quando os Domain Name são mudados demasiado; o nome de domínio original é considerado na entrada de ITLRecovery a fim assegurar-se de que a chave da recuperação não mude. _a única vez que ITLRecovery certificado dever mudar quando expirar devido de cinco anos validez e dever estar regenerar.

Os keypairs da recuperação ITL podem ser regenerados com o CLI ou a página de administração do OS. Os Telefones IP não são restaurados quando o certificado de ITLRecovery é regenerado no editor ou em algum dos assinantes. Uma vez que o certificado de ITLRecovery foi regenerado, o arquivo ITL não atualiza até que o serviço TFTP esteja reiniciado. Após a regeneração do certificado de ITLRecovery no editor, reinicie o serviço TFTP em cada nó que dirige o serviço TFTP no conjunto a fim atualizar a entrada de ITLRecovery no arquivo ITL com o certificado novo. A etapa final é restaurar todos os dispositivos do **sistema > parâmetros de empreendimento** e usar o botão reset a fim fazer a toda a transferência dos dispositivos o arquivo novo ITL que contém o certificado novo de ITLRecovery.

Suporte a recuperação ITL

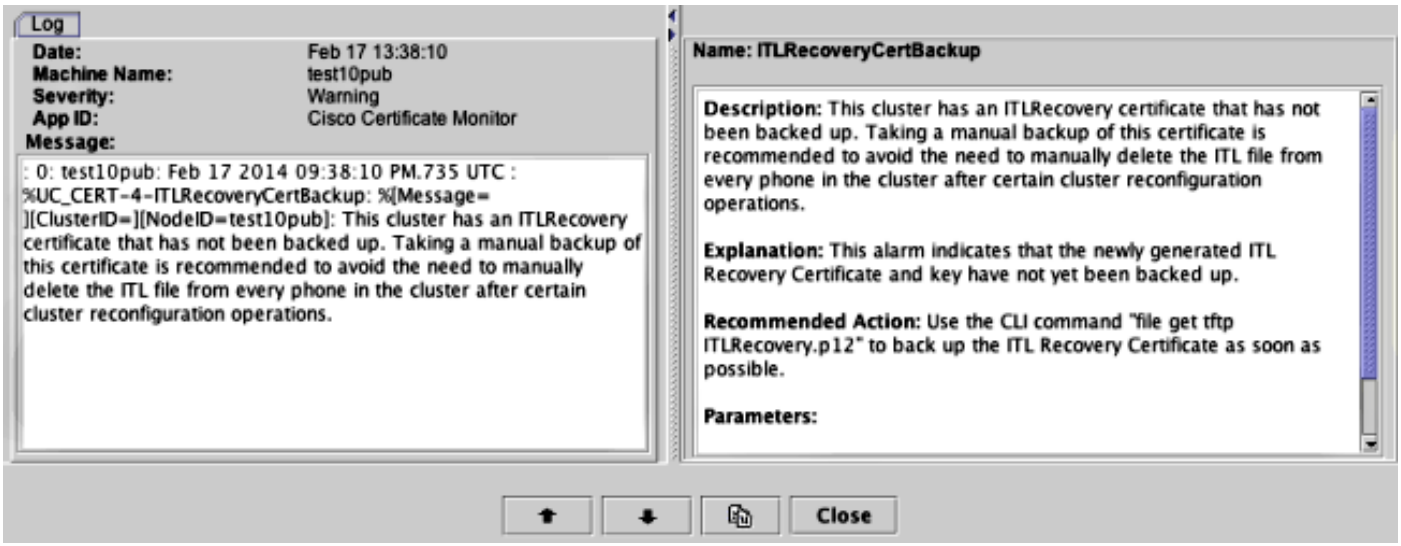
A chave da recuperação ITL está exigida a fim recuperar telefones quando entram em um estado não-confiável. Devido a isto, os alertas novos da ferramenta do monitoramento em tempo real (RTMT) estão gerados diariamente até que a chave da recuperação ITL esteja suportada. Um backup do sistema da Recuperação de desastres (DR) não basta parar os alertas. Embora um backup seja recomendado a fim salvar a chave da recuperação ITL, um backup manual do arquivo-chave é precisado também.

A fim suportar a chave da recuperação, o início de uma sessão ao CLI do editor e incorporar o **arquivo obtém o** comando de **tftp ITLRecovery.p12**. Um servidor SFTP é precisado a fim salvar o arquivo a como mostrado aqui. Os Nós do subscritor não têm um arquivo de recuperação ITL, assim que se você emite o **arquivo obtêm o** comando de **tftp ITLRecovery.p12 em um** subscritor, ele conduzem ao **arquivo não 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
```

Até que o backup manual esteja executado do CLI a fim suportar o arquivo ITLRecovery.p12, um aviso está imprimido no CiscoSyslog (log de aplicativo event viewer) cada dia como mostrado aqui. Um email diário pôde igualmente ser recebido até que o backup manual esteja executado se a notificação de Email está permitida da página de administração do OS, **Segurança > monitor do certificado**.



Quando um backup DR contiver o ITLRecovery, recomenda-se armazenar ainda o arquivo ITLRecovery.p12 em um local segura caso que os arquivos de backup são perdidos ou corrompidos ou a fim ter a opção para restaurar o arquivo ITL sem a necessidade de restaurar de um backup. Se você tem o arquivo ITLRecovery.p12 do editor salvar, igualmente permite que o editor esteja reconstruído sem um backup com o uso a opção da restauração DR restaurar o base de dados de um susbcriber e restabelecer a confiança entre os telefones e server CUCM restaurando a ITL com a opção do **remotekey da restauração ITL dos utils**.

Recorde que se o editor é reconstruído, a senha de segurança do conjunto deve ser a mesma que o editor de onde o arquivo ITLRecovery.p12 foi tomado porque o arquivo ITLRecovery.p12 é senha protegida com uma senha baseada fora da senha de segurança do conjunto. Por este motivo, se a senha de segurança do conjunto é mudada, o alerta RTMT que indica que o arquivo ITLRecovery.p12 não esteve suportado está restaurado e provocado o diário até que o arquivo ITLRecovery.p12 novo estado salvar com o **arquivo obtiver o** comando de **tftp ITLRecovery.p12**.

Verificar

A característica da restauração ITL do volume trabalha somente se os telefones têm uma ITL instalada que contenha a entrada de ITLRecovery. A fim verificar que o arquivo ITL instalado nos telefones contém a entrada de ITLRecovery, incorpore o comando **ITL da mostra do** CLI em cada um dos servidores TFTP encontrar a soma de verificação do arquivo ITL. A saída do comando **ITL da mostra** indica a soma de verificação:

```
admin:show itl
```

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

A soma de verificação é diferente em cada servidor TFTP porque cada server tem seu próprio **certificado callmanager.pem em** seu arquivo ITL. A soma de verificação ITL da ITL instalada no telefone pode ser encontrada se você vê a ITL no telefone própria sob a **configuração do > segurança dos** ajustes **> a lista da confiança, do** página da web do telefone, ou do alarme de DeviceTLInfo relatado pelos telefones que executam um firmware mais novo.

A maioria de telefones que executam a versão de firmware 9.4(1) ou um relatório mais atrasado a mistura SHA1 de sua ITL a CUCM com o alarme de DeviceTLInfo. A informação enviada pelo telefone pode ser vista no log de aplicativo event viewer de RTMT e comparado à mistura SHA1 da mistura ITL dos servidores TFTP os telefones usam-se a fim encontrar todos os telefones que não tiverem a ITL atual instalada, que contém a entrada de ITLRecovery.

Caveats

- CSCun18578 - A restauração localkey/remotekey ITL falha em determinadas encenações
- CSCun19112 - A ITL restaurou o erro do remotekey no tipo da autenticação inválida SFTP