Aprimoramentos de ITL do Unified Communications Manager na versão 10.0(1)

Contents

Introduction

Este documento descreve um novo recurso no Cisco Unified Communications Manager (CUCM) versão 10.0(1) que permite a redefinição em massa de arquivos da lista de confiança de identidade (ITL) em telefones IP Cisco Unified. O recurso de redefinição de ITL em massa é usado quando os telefones não confiam mais no sinalizador de arquivos ITL e também não podem autenticar o arquivo ITL fornecido pelo serviço TFTP localmente ou com o uso do Trust Verification Service (TVS).

Background

A capacidade de redefinir em massa arquivos ITL evita a necessidade de executar uma ou várias dessas etapas para restabelecer a confiança entre os telefones IP e os servidores CUCM.

- Restaurar de um backup para carregar um arquivo ITL antigo confiável pelos telefones
- Alterar os telefones para usar um servidor TFTP diferente
- Exclua o arquivo ITL do telefone manualmente pelo menu de configurações
- A fábrica redefiniu o telefone nas configurações de evento para que o acesso seja desativado para apagar o ITL

Este recurso não se destina a mover telefones entre clusters; para essa tarefa, use um dos métodos descritos em Migração de Telefones IP entre Clusters com CUCM 8 e Arquivos ITL. A operação de redefinição de ITL é usada somente para restabelecer a confiança entre os telefones IP e o cluster CUCM quando eles perderam seus pontos de confiança.

Outro recurso relacionado à segurança disponível na versão 10.0(1) do CUCM que não é abordado neste documento é a Lista de Confiança de Certificado Sem Tokenless (CTL). O CTL sem tokenless substitui os tokens de segurança USB de hardware por um token de software usado para habilitar a criptografia nos servidores e endpoints do CUCM. Para obter informações adicionais, consulte o documento Segurança do telefone IP e CTL (Certificate Trust List).

Informações adicionais sobre os arquivos ITL e segurança por padrão podem ser encontradas no documento Segurança por padrão do Communications Manager e Operação e solução de problemas do ITL.

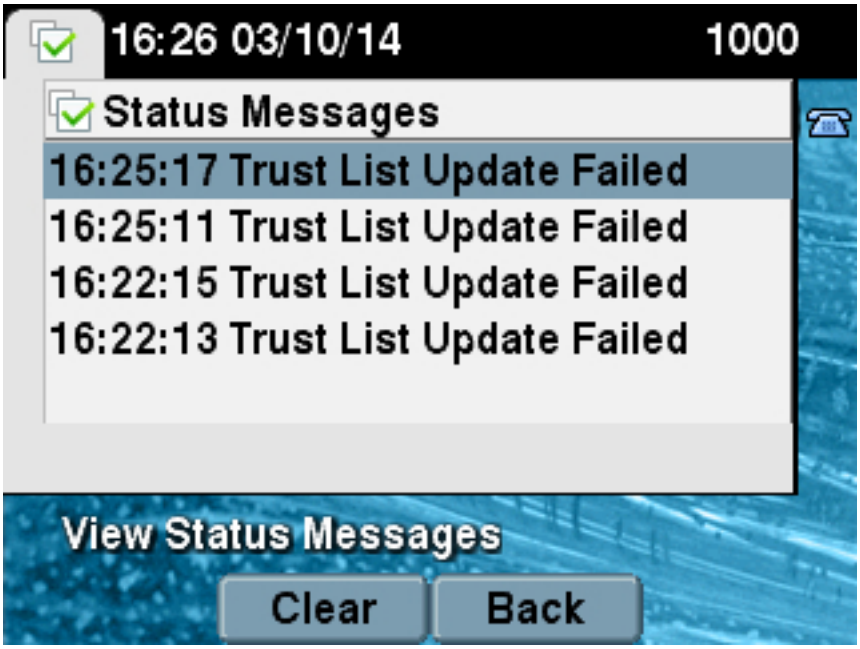
Sintomas do problema

Quando os telefones estão em um estado **bloqueado** ou **não confiável**, eles não aceitam o arquivo ITL ou a configuração TFTP fornecida pelo serviço TFTP. Qualquer alteração de configuração contida no arquivo de configuração TFTP não é aplicada ao telefone. Alguns exemplos de configurações contidas no arquivo de configuração TFTP são:

- Acesso às configurações
- Acesso à Web
- Acesso Secure Shell (SSH)
- Analisador de porta comutada (SPAN - Switched Port Analyzer) para porta de PC

Se qualquer uma dessas configurações for alterada para um telefone na página CCM Admin e, depois que o telefone for redefinido, as alterações não entrarão em vigor, o telefone poderá não confiar no servidor TFTP. Outro sintoma comum é que quando você acessa o diretório corporativo ou outros serviços de telefone, a mensagem **Host Not Found (Host não encontrado)** é exibida. Para verificar se o telefone está em um estado bloqueado ou não confiável, verifique as mensagens de status do telefone do próprio telefone ou da página da Web do telefone para ver se uma mensagem **Trust List Update Failed** é exibida. A mensagem **Falha na Atualização do ITL** é um indicador de que o telefone está em um estado bloqueado ou não confiável porque ele não conseguiu autenticar a lista confiável com seu ITL atual e não conseguiu autenticá-lo com TVS.

A mensagem **Trust List Update Failed (Falha na atualização da lista de confiança)** pode ser vista do próprio telefone se você navegar para **Settings > Status > Status Messages (Configurações > Status > Mensagens de status)**:



A mensagem **Trust List Update Failed** também pode ser vista na página do telefone na Web nas **Mensagens de status** como mostrado aqui:

Solução - Redefinição em massa de ITL

O CUCM Versão 10.0(1) usa uma chave adicional que pode ser usada para restabelecer a confiança entre os telefones e os servidores CUCM. Essa nova chave é a chave de recuperação ITL. A chave de recuperação ITL é criada durante a instalação ou atualização. Essa chave de recuperação não é alterada quando o nome do host é alterado, alterações de DNS ou outras alterações que podem levar a problemas em que os telefones entram em um estado em que não confiam mais no assinante de seus arquivos de configuração.

O comando CLI **itl reset** do novo **utilitário** pode ser usado para restabelecer a confiança entre um telefone ou telefones e o serviço TFTP no CUCM quando os telefones estão em um estado em que a mensagem **Trust List Update Failed** é exibida. O comando **utils itl reset**:

1. Pega o arquivo ITL atual do nó do editor, retira a assinatura do arquivo ITL e assina o conteúdo do arquivo ITL novamente com a chave privada de Recuperação ITL.
2. Copia automaticamente o novo arquivo ITL para os diretórios TFTP em todos os nós TFTP ativos no cluster.
3. Reinicializa automaticamente os serviços TFTP em cada nó em que o TFTP é executado.

O administrador deve redefinir todos os telefones. A redefinição faz com que os telefones

solicitem o arquivo ITL na inicialização do servidor TFTP e o arquivo ITL recebido pelo telefone é assinado pela chave ITLRecovery em vez da chave privada **callmanager.pem**. Há duas opções para executar uma redefinição de ITL: **utils itl reset localkey** e **utils itl reset remotekey**. O comando ITL reset só pode ser executado do editor. Se você emitir uma redefinição de ITL de um assinante, isso resultará na mensagem **Isto não é um nó do editor**. Exemplos de cada comando são detalhados nas próximas seções.

ITLRecovery com a chave de recuperação local

A opção localkey usa a chave privada de recuperação ITL contida no arquivo ITLRecovery.p12 presente no disco rígido do Publisher como o novo assinante de 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 de recuperação remota

A opção remotekey permite que o servidor SFTP externo do qual o arquivo ITLRecovery.p12 foi salvo seja 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
```

> **Note**: Se uma redefinição de ITL for feita com a opção remotekey, a localkey (no arquivo do disco) no editor será substituída pela tecla remota.

Verifique o assinante atual com o comando "show itl"

Se você visualizar o arquivo ITL com o comando **show itl** antes de emitir um comando ITL reset, ele mostrará que o ITL contém uma entrada **ITLRECOVERY_*<publisher_hostname>***. Cada arquivo ITL que é servido por qualquer servidor TFTP no cluster contém esta entrada de recuperação ITL do editor. A saída do comando **show itl** é tirada do editor neste exemplo. O token usado para assinar o ITL está em negrito:

```
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 se a chave de recuperação ITLR foi usada

Se você visualizar o arquivo ITL com o comando **show itl** depois de executar uma redefinição ITL, ele mostrará que a entrada ITLRecovery assinou o ITL como mostrado aqui. O ITLRecovery permanece o signatário do ITL até que o TFTP seja reiniciado, quando o **callmanager.pem** ou certificado TFTP é usado para assinar o ITL novamente.

```
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.
```

Melhorias para reduzir a possibilidade de telefones perderem a confiança

Além do recurso de redefinição ITL, o CUCM Versão 10.0(1) inclui recursos de administrador que ajudam a impedir que os telefones entrem em um estado não confiável. Os dois pontos de confiança que o telefone tem são o certificado TVS (**TVS.pem**) e o certificado TFTP (**callmanager.pem**). No ambiente mais simples com apenas um servidor CUCM, se um administrador regenerar o certificado **callmanager.pem** e o certificado **TVS.pem** um logo após o outro, o telefone será redefinido e, durante a inicialização, será exibida a mensagem **Falha na atualização da lista de confiança**. Mesmo com uma redefinição automática de dispositivo enviada do CUCM para o telefone devido a um certificado contido no ITL que é regenerado, o telefone pode digitar um estado em que não confia no CUCM.

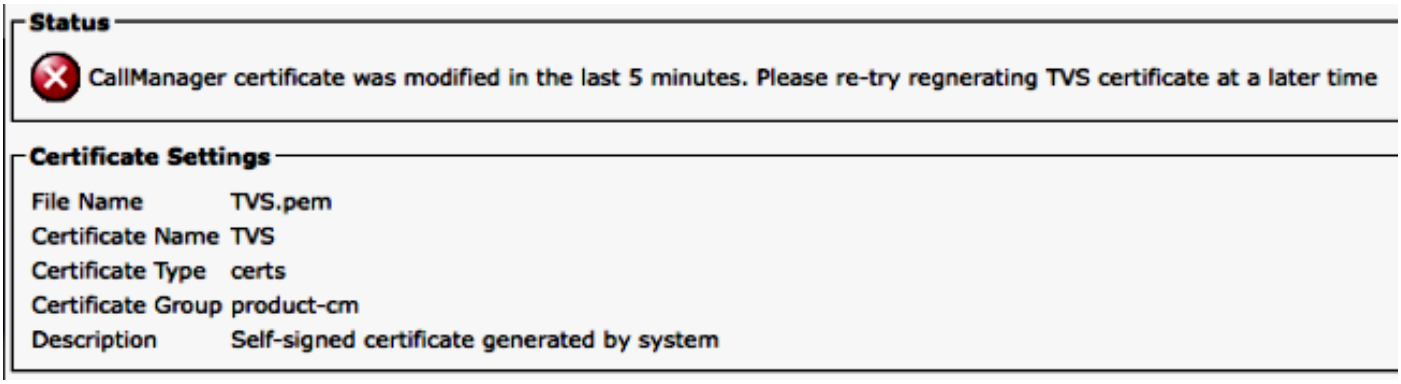
Para ajudar a evitar o cenário em que vários certificados são regenerados ao mesmo tempo (normalmente alteração de nome de host ou modificações de nome de domínio DNS), o CUCM agora tem um temporizador de espera. Quando um certificado é regenerado, o CUCM impede que o administrador regenere outro certificado no mesmo nó em cinco minutos após a regeneração do certificado anterior. Esse processo faz com que os telefones sejam redefinidos ao regenerar o primeiro certificado e eles devem ser registrados e de backup antes que o próximo certificado seja regenerado.

Independentemente de qual certificado é gerado primeiro, o telefone tem seu método secundário para autenticar arquivos. Detalhes adicionais sobre esse processo podem ser encontrados em Segurança do Communications Manager por padrão e Operação e Troubleshooting do ITL.

Esta saída mostra uma situação em que o CUCM impede que o administrador regenere outro certificado dentro de cinco minutos de uma regeneração de certificado anterior conforme exibido na 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 vista na página de administração do sistema operacional (SO), como mostrado aqui:



A chave de recuperação ITL do editor é a única em uso pelo cluster inteiro, mesmo que cada nó tenha seu próprio certificado de recuperação ITLR emitido para o Nome Comum (CN) de **ITLRecovery_*<node name>***. A chave ITLRecovery do editor é a única usada nos arquivos ITL para todo o cluster, conforme visto no comando **show itl**. É por isso que a única entrada **ITLRecovery_*<hostname>*** vista em um arquivo ITL contém o nome de host do editor.

Se o nome de host do editor for alterado, a entrada ITLRecovery no ITL continuará a mostrar o nome de host antigo do editor. Isso é feito intencionalmente porque o arquivo ITLRecovery nunca deve ser alterado para garantir que os telefones sempre confiem na recuperação do ITL.

Isso se aplica quando os nomes de domínio são alterados também; o nome de domínio original é visto na entrada ITLRecovery para garantir que a chave de recuperação não seja alterada. A única vez que o certificado de recuperação ITLR deve ser alterado é quando expira devido à validade de cinco anos e deve ser regenerado.

Os pares de chaves de recuperação ITL podem ser regenerados com a página CLI ou a página Administração do SO. Os telefones IP não são redefinidos quando o certificado ITLRecovery é regenerado no editor ou em qualquer um dos assinantes. Depois que o certificado de recuperação ITLR tiver sido regenerado, o arquivo ITL não será atualizado até que o serviço TFTP seja reiniciado. Após a regeneração do certificado de recuperação ITLR no editor, reinicie o serviço TFTP em cada nó que executa o serviço TFTP no cluster para atualizar a entrada de recuperação ITLR no arquivo ITL com o novo certificado. A etapa final é redefinir todos os dispositivos de **System > Enterprise Parameters** e usar o botão reset para fazer com que todos os dispositivos baixem o novo arquivo ITL que contém o novo certificado de recuperação ITLR.

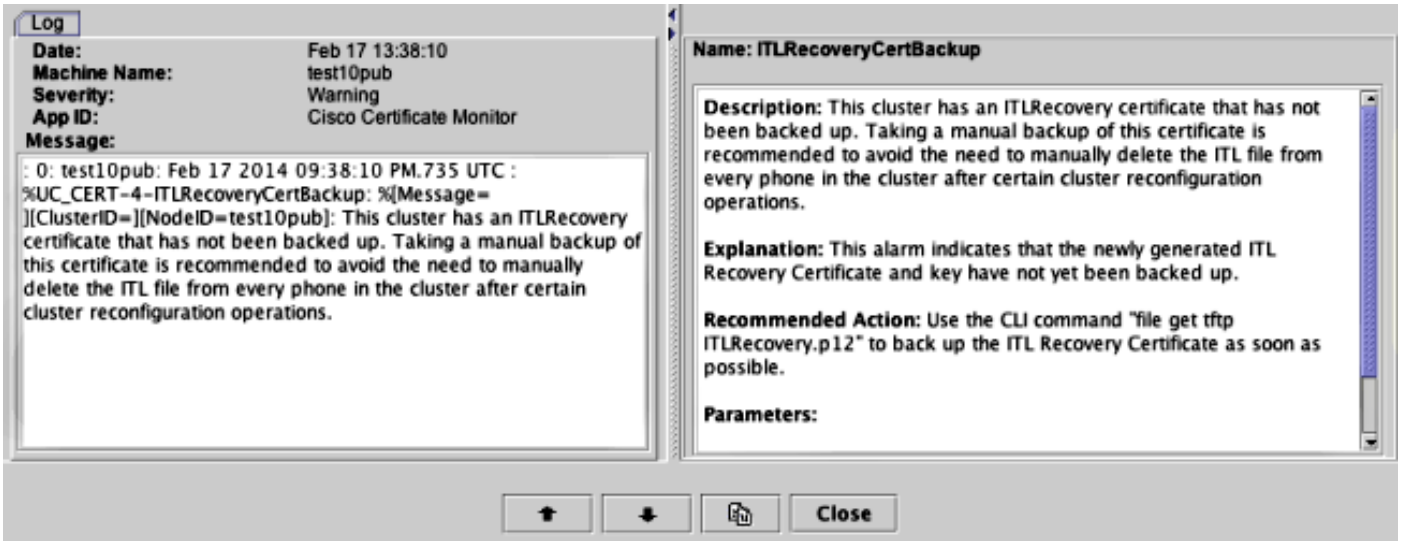
Fazer backup da recuperação do ITL

A chave de recuperação ITL é necessária para recuperar telefones quando eles entram em um estado não confiável. Devido a isso, novos alertas da Real-Time Monitoring Tool (RTMT) são gerados diariamente até que seja feito o backup da chave de recuperação do ITL. Um backup do Sistema de Recuperação de Desastre (DRS) não é suficiente para interromper os alertas. Embora um backup seja recomendado para salvar a chave de recuperação ITL, também é necessário um backup manual do arquivo de chave.

Para fazer backup da chave de recuperação, faça login na CLI do editor e insira o comando **file get tftp ITLRecovery.p12**. Um servidor SFTP é necessário para salvar o arquivo no, como mostrado aqui. Os nós do assinante não têm um arquivo de recuperação ITL, portanto, se você executar o comando **get tftp ITLRecovery.p12 em um assinante, o resultado será que o arquivo não foi 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 seja executado a partir da CLI para fazer backup do arquivo ITLRecovery.p12, um aviso é impresso no CiscoSyslog (Event Viewer - Application Log) todos os dias, como mostrado aqui. Um e-mail diário também pode ser recebido até que o backup manual seja executado se a notificação por e-mail for ativada na página Administração do SO, **Segurança > Monitor de certificado**.



Embora um backup de DRS contenha ITLRecovery, recomenda-se ainda armazenar o arquivo ITLRecovery.p12 em um local seguro, caso os arquivos de backup sejam perdidos ou corrompidos ou para ter a opção de redefinir o arquivo ITL sem a necessidade de restaurar a partir de um backup. Se você tiver o arquivo ITLRecovery.p12 do editor salvo, ele também permitirá que o editor seja reconstruído sem um backup com a opção de restauração DRS para restaurar o banco de dados de um assinante e restabelecer a confiança entre os telefones e os servidores CUCM, redefinindo o ITL com a opção **utils itl reset remotekey**.

Lembre-se de que, se o editor for recriado, a senha de segurança do cluster deverá ser a mesma do editor do qual o arquivo ITLRecovery.p12 foi retirado, pois o arquivo ITLRecovery.p12 é protegido por senha com uma senha baseada na senha de segurança do cluster. Por esse motivo, se a senha de segurança do cluster for alterada, o alerta RTMT que indica que o backup do arquivo ITLRecovery.p12 não foi feito será redefinido e dispara diariamente até que o novo arquivo ITLRecovery.p12 seja salvo com o comando **file get tftp ITLRecovery.p12**.

Verificar

O recurso de redefinição de ITL em massa só funciona se os telefones tiverem um ITL instalado que contenha a entrada ITLRecovery. Para verificar se o arquivo ITL instalado nos telefones contém a entrada ITLRecovery, insira o comando **show itl** na CLI em cada um dos servidores TFTP para encontrar a soma de verificação do arquivo ITL. A saída do comando **show itl** exibe 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 servidor tem seu próprio certificado **callmanager.pem** em seu arquivo ITL. A soma de verificação ITL do ITL instalado no telefone pode ser encontrada se você visualizar o ITL no próprio telefone em **Configurações > Configuração de segurança > Lista de confiança**, na página da Web do telefone ou no alarme DeviceTLInfo relatado por telefones que executam firmware mais recente.

A maioria dos telefones que executam o firmware versão 9.4(1) ou posterior reportam o hash SHA1 de seu ITL para o CUCM com o alarme DeviceTLInfo. As informações enviadas pelo telefone podem ser visualizadas no Event Viewer - Application Log da RTMT e comparadas ao hash SHA1 do hash ITL dos servidores TFTP usados pelos telefones para encontrar telefones que não têm o ITL instalado atualmente, que contém a entrada de recuperação ITLR.

Caveats

- CSCun18578 - falha de chave local/tecla remota de redefinição ITL em determinados cenários
- CSCun19112 - erro ITL reset remotekey no tipo de autenticação de SFTP inválido