10.0(1)版中的统一通信管理器ITL增强功能

目录

简介

本文档介绍Cisco Unified Communications Manager(CUCM)版本10.0(1)中的一项新功能，该功能可在Cisco Unified IP电话上批量重置身份信任列表(ITL)文件。当电话不再信任ITL文件签名者，并且无法在本地或使用信任验证服务(TVS)对TFTP服务提供的ITL文件进行身份验证时，会使用批量ITL重置功能。

背景

批量重置ITL文件的功能可防止执行以下一个或多个步骤以在IP电话和CUCM服务器之间重新建立信任。

- 从备份中恢复，以上传电话信任的旧ITL文件
- 更改电话以使用不同的TFTP服务器
- 通过设置菜单手动从电话中删除ITL文件
- 出厂时在事件设置中重置电话，以便禁用访问以清除ITL

此功能不用于在集群之间移动电话；对于该任务，请使用在CUCM 8和ITL文件[的集群之间迁移IP电话中描述的方法之一](#)。ITL重置操作仅用于在IP电话和CUCM集群失去信任点时重新建立信任。

CUCM版本10.0(1)中提供的与安全相关的功能（本文档未涵盖）是无令牌证书信任列表(CTL)。 无令牌CTL将硬件USB安全令牌替换为用于在CUCM服务器和终端上启用加密的软件令牌。有关其他信息，请参阅[IP电话安全和CTL（证书信任列表）](#)文档。

有关ITL文件和默认安全的其他信息，请参阅Communications Manager Security By [Default和ITL Operation and Troubleshooting文档中的](#)信息。

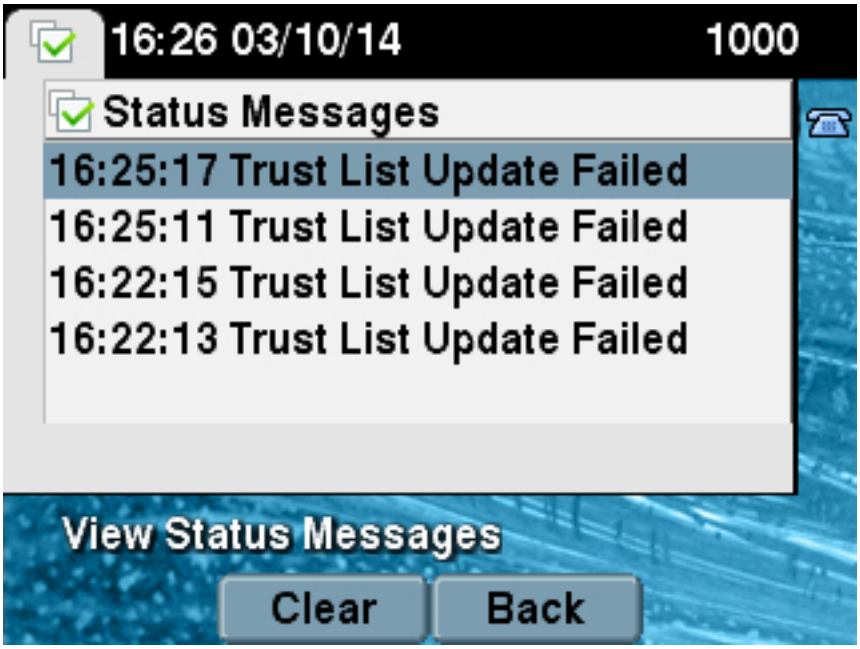
问题症状

当电话处于锁定**或**不受信**任**状态时，它们不接受TFTP服务提供的ITL文件或TFTP配置。TFTP配置文件中包含的任何配置更改都不会应用到电话。TFTP配置文件中包含的一些设置示例包括：

- 设置访问
- Web 访问
- 安全外壳(SSH)访问
- 交换端口分析器(SPAN)到PC端口

如果在CCM Admin页面上更改了电话的这些设置中的任何一项，并且重置电话后，更改不会生效，电话可能不信任TFTP服务器。另一个常见症状是当您访问公司目录或其他电话服务时，系统会显示**"Host Not Found(找不到主**机)"。要验证电话是否处于锁定或不受信任状态，请检查电话本身或电话网页中的电话状态消息，以查看是否显示"信任列表更新失败"消息。**ITL更新失败**消息表明电话处于锁定或不受信任状态，因为它未能使用其当前ITL对信任列表进行身份验证，并且未能使用TVS对其进行身份验证。

如果**导航至"设置">"状态">**"状态消息"，则可以从电话本**身看到"信任列表更新失败**"：



也可**以从"状态**消息"的电话网页中看到"信任列表更**新失败**"消息，如下所示：

解决方案 — 批量ITL重置

CUCM版本10.0(1)使用可用于重新建立电话和CUCM服务器之间信任的附加密钥。此新密钥是ITL恢复密钥。ITL恢复密钥在安装或升级期间创建。当主机名更改、DNS更改或执行其他更改时，此恢复密钥不会更改，这可能导致电话进入不再信任其配置文件签名者的状态。

当电话处于显示**Trust List Update Failed消息的状态时，可使用新的utils itl reset** CLI命令在电话或电话与CUCM上的TFTP服务之间重新建立信任。utils itl reset**命令：**

1. 从发布方节点获取当前ITL文件，删除ITL文件的签名，并使用ITL恢复私钥再次对ITL文件的内容进行签名。
2. 自动将新的ITL文件复制到集群中所有活动TFTP节点上的TFTP目录。
3. 在运行TFTP的每个节点上自动重新启动TFTP服务。

然后，管理员必须重置所有电话。重置会使电话在从TFTP服务器启动时请求ITL文件，并且电话收到的ITL文件由ITLRecovery密钥而不是**callmanager.pem私**钥签名。运行ITL重置有两个选项：**utils itl reset localkey和utils itl reset remotekey**。ITL reset命令只能从发布方运行。如果从订用者发出ITL重置，则会显示“**This is not a Publisher Node（这不是发布者节点）**”消息。每个命令的示例将在后续部分详细介绍。

ITLR使用本地恢复密钥进行恢复

localkey选项使用发布服务器硬盘上存在的ITLRecovery.p12文件中包含的ITL恢复私钥作为新的ITL文件签名者。

```
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
```

ITLR使用远程恢复密钥进行恢复

remotekey选项允许指定从中保存ITLRecovery.p12文件的外部SFTP服务器。

```
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
```

注意：如果使用remotekey选项完成ITL重置，则发布服务器上的localkey（磁盘文件上）将替换为remotekey。

使用“show itl”命令验证当前签名者

如果在发出ITL重置命令之**前使**用show itl命令查看ITL文件，则它显示ITL包含**ITLRECOVERY_*<publisherhostname>***条目。集群中任何TFTP服务器提供的每个ITL文件都包含来自发布方的此ITL恢复条目。在本例中，**show itl**命令的输出取自发布者。用于签署ITL的令牌以粗体显示：

```
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.
```

验证ITLRecovery密钥已使用

如果在执行ITL重置后使用**show itl**命令查看ITL文件，则显示ITLRecovery条目已对ITL签名，如下所示。ITLRecovery在重新启动TFTP之前仍是ITL的签名者，此时会使用**callmanager.pem**或TFTP证书来再次对ITL签名。

```
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.
```

增强功能，降低电话失去信任的可能性

除ITL重置功能外，CUCM 10.0(1)版还包含有助于防止电话进入不受信任状态的管理员功能。电话具有的两个信任点是TVS证书(**TVS.pem**)和TFTP证书(**callmanager.pem**)。 在仅使用一个CUCM服务器的最简单环境中，如果管理员先后重新生成**callmanager.pem**证书和**TVS.pem**证书，电话将重置，并在启动时显示**Trust List Update Failed**消息。即使由于ITL中包含的证书而从CUCM自动将设备重置发送到电话，电话也可以进入不信任CUCM的状态。

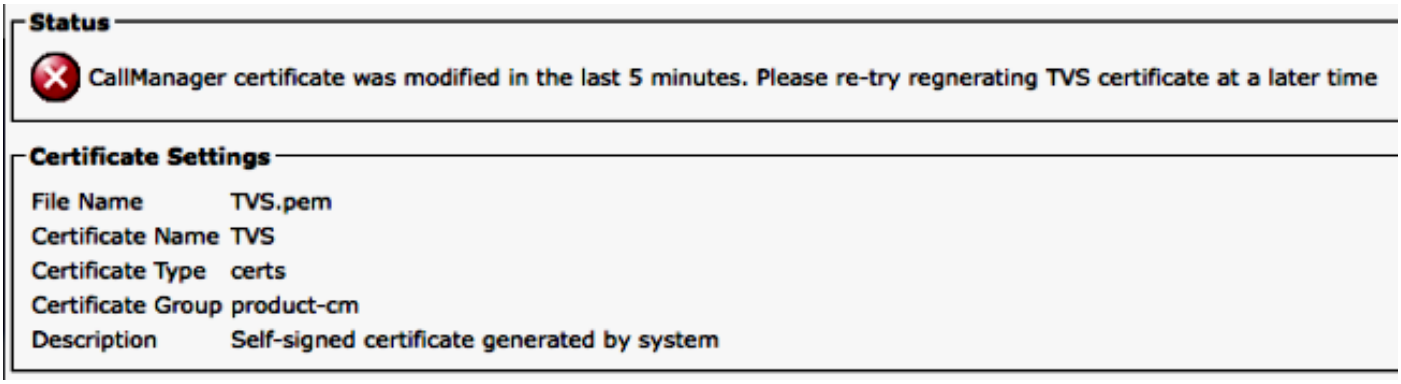
为了帮助防止同时重新生成多个证书（通常是主机名更改或DNS域名修改）的情况，CUCM现在具有保持计时器。重新生成证书时，CUCM会阻止管理员在先前证书重新生成后的五分钟内在同一节点上重新生成另一个证书。此过程会导致在重新生成第一个证书时重置电话，并且在重新生成下一个证书之前应备份和注册电话。

无论首先生成哪个证书，电话都有其辅助方法来验证文件。有关此流程的其他详细信息，请参阅 Communications Manager Security Default和ITL Operation and Troubleshooting。

此输出显示一种情况，即CUCM在从CLI查看的先前证书重新生成后的五分钟内阻止管理员重新生成另一个证书：

```
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
```

从操作系统(OS)管理页面可以看到相同的消息，如下所示：



发布者ITL恢复密钥是整个集群中唯一使用的密钥，即使每个节点都有自己的ITLRecovery证书颁发给ITLRecovery_<节点名**称>的公*用名(CN)*。发布方ITLRecovery密钥是从show itl命令中看到的整个集群的ITL文件中唯一使**用的**密钥。这就是为什么在ITL文**件中看*到的***唯一ITLRecovery_<hostname>条目包含发布者的主机名的原因。

如果发布者的主机名更改，ITL中的ITLRecovery条目将继续显示发布者的旧主机名。这是有意为之的，因为ITLRecovery文件永远不应更改，以确保电话始终信任ITL恢复。

当域名也发生更改时，此情况也适用；在ITLRecovery条目中可以看到原始域名，以确保恢复密钥不会更改。ITLRecovery证书应更改的唯一时间是证书因五年有效期而到期，必须重新生成。

ITL恢复密钥对可以通过CLI或OS Administration页面重新生成。在发布者或任何订阅者上重新生成ITLRecovery证书时，IP电话不会重置。重新生成ITLRecovery证书后，ITL文件在重新启动TFTP服务之前不会更新。在发布方上重新生成ITLRecovery证书后，在集群中运行TFTP服务的每个节点上重新启动TFTP服务，以便使用新证书更新ITL文件中的ITLRecovery条目。最后一步是从**System > Enterprise Parameters**重置所有设备，并使用重置按钮，以使所有设备下载包含新ITLRecovery证书的新ITL文件。

备份ITL恢复

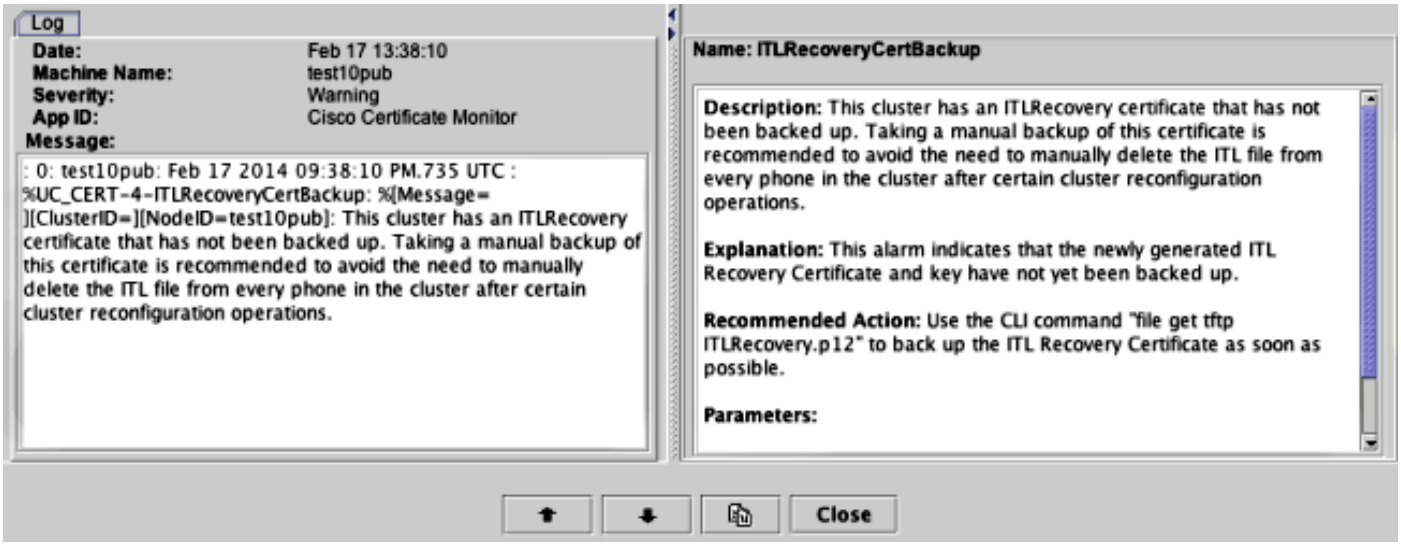
当电话进入不可信状态时，需要使用ITL恢复密钥才能恢复电话。因此，在备份ITL恢复密钥之前，每天都会生成新的实时监控工具(RTMT)警报。灾难恢复系统(DRS)备份不足以停止警报。虽然建议备份以保存ITL恢复密钥，但也需要手动备份密钥文件。

要备份恢复密钥，请登录发布方的CLI并输入**file get tftp ITLRecovery.p12命**令。要将文件保存到，需要SFTP服务器，如下所示。用户节点没有ITL恢复文件，因此，如果在用户上发出**file get tftp ITLRecovery.p12**命令，将导致**找不到文件**。

```
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
```

在从CLI执行手动备份以备份ITLRecovery.p12文件之前，CiscoSyslog（事件查看器 — 应用程序日志）每天都会显示警告，如下所示。如果从OS Administration页面“Security”>“Certificate Monitor”启用邮件通知，则在执行手动备份之前，也可能会收到每**日电子邮件**。



当DRS备份包含ITLRecovery时，建议仍将ITLRecovery.p12文件存储在安全位置，以防备文件丢失或损坏，或者为了能够选择重置ITL文件而不需要从备份中恢复。如果保存了发布方的ITLRecovery.p12文件，它还允许使用DRS恢复选项从订阅服务器恢复数据库，并通过使用utils itl reset remotekey选项重置ITL来重新建立电话和CUCM服务器之间的信任，从而在不备份的情况下重建发布方。

请记住，如果重建发布者，则集群安全密码应与从其中提取ITLRecovery.p12文件的发布者相同，因为ITLRecovery.p12文件受密码保护，密码基于集群安全密码。因此，如果更改集群安全密码，则重置RTMT警报（指示ITLRecovery.p12文件尚未备份），并每天触发，直到新的ITLRecovery.p12文件与**file get tftp ITLRecovery.p12**命令一起保存。

验证

批量ITL重置功能仅在电话安装了包含ITLRecovery条目的ITL时有效。要验证安装在电话上的ITL文件是否包含ITLRecovery条目，请在每台TFTP服务器的CLI中输入**show itl**命令，以查找ITL文件的校验和。show itl命令的**输出**显示校验和：

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

每个TFTP服务器上的校验和不同，因为每个服务器的ITL文件中**都有其自**己的callmanager.pem证书。如果在**Settings > Security Configuration > Trust List**下查看电话本身上的ITL，或从电话网页或运行较新固件的电话报告的DeviceTLInfo警报，则可以找到电话上安装的ITL的ITL校验和。

大多数运行固件版本9.4(1)或更高版本的电话使用DeviceTLInfo警报将其ITL的SHA1哈希值报告给

CUCM。电话发送的信息可在事件查看器 — 来自RTMT的应用日志中查看，并与电话使用的TFTP服务器的ITL散列的SHA1散列进行比较，以查找未安装当前ITL（包含ITLRecovery条目）的任何电话。

注意事项

- CSCun18578 - ITL reset localkey/remotekey在某些情况下失败
- CSCun19112 - SFTP错误身份验证类型中的ITL reset remotekey错误