統一通訊管理器10.0(1)版中的ITL增強功能

目錄

簡介

本檔案介紹Cisco Unified Communications Manager(CUCM)版本10.0(1)中的一項新功能，該功能可在Cisco Unified IP電話上批次重置身份信任清單(ITL)檔案。當電話不再信任ITL檔案簽名者並且也無法對TFTP服務在本地或利用信任驗證服務(TVS)提供的ITL檔案進行驗證時，使用批次國際交易日誌重置功能。

背景

批次重設ITL檔案的能力可防止在IP電話和CUCM伺服器之間重新建立信任需要執行其中的一個或多個步驟。

- 從備份恢復，以便上傳電話信任的舊ITL檔案
- 更改電話以便使用不同的TFTP伺服器
- 通過設定選單手動從電話刪除國際交易日誌檔案
- 出廠時重置事件設定中的電話，以便禁用訪問以清除ITL

此功能不適用於在集群之間行動電話；對於該任務，請使用使用CUCM 8和ITL檔案在集群之間遷移IP電話中介紹的方法之一。ITL重置操作僅用於在IP電話和CUCM集群失去信任點時重建信任。

CUCM版本10.0(1)中提供的另一個與安全性相關的功能是無標籤證書信任清單(CTL)，本文檔未介紹該功能。 無標籤CTL用軟體令牌代替硬體USB安全令牌，用於在CUCM伺服器和終端上啟用加密。如需其他資訊，請參閱IP電話安全和CTL（憑證信任清單）檔案。

有關國際交易日誌檔案和預設安全性的其他資訊，請參閱通訊管理器預設安全和國際交易日誌運行和故障排除文檔。

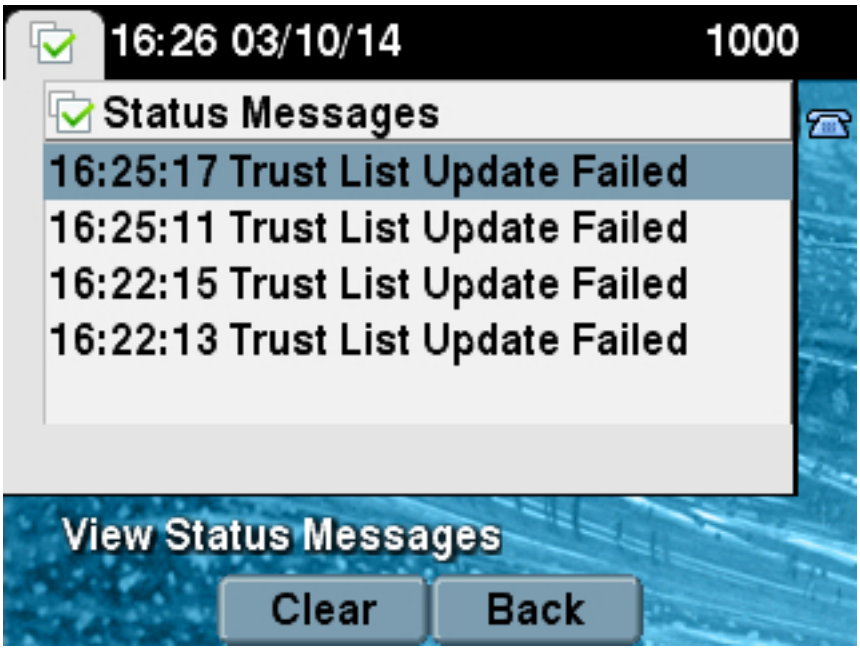
問題症狀

當電話處於**locked**或**untrusted**狀態時，他們不接受TFTP服務提供的ITL檔案或TFTP配置。TFTP配置檔案中包含的任何配置更改都不會應用到電話。TFTP配置檔案中包含的一些設定示例包括：

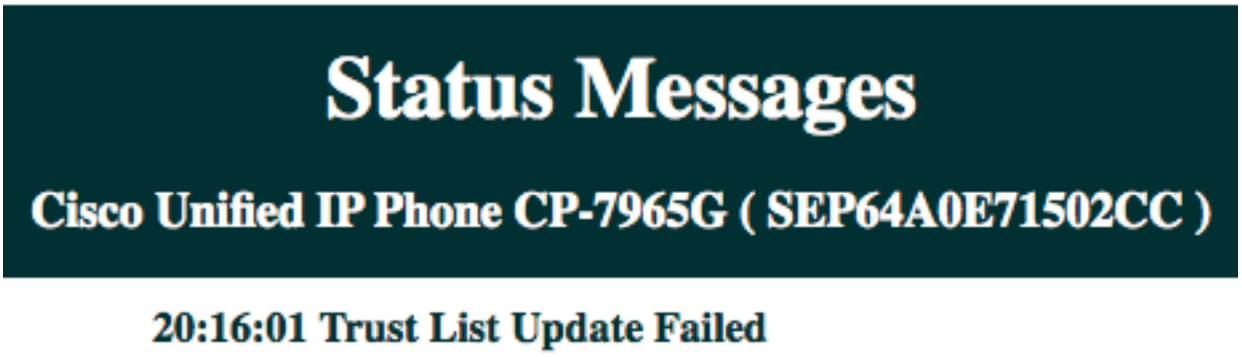
- 設定訪問
- Web訪問
- 安全殼層(SSH)存取
- 交換器連線埠分析器(SPAN)到PC連線埠

如果電話在CCM Admin頁面上更改了其中任何設定，並且重置電話後，這些更改不再生效，則該電話可能不會信任TFTP伺服器。另一個常見症狀是當您訪問公司目錄或其他電話服務時，系統會顯示資訊**Host Not Found**。若要確認電話是否處於鎖定或不受信任狀態，請檢查電話本身或電話網頁上的電話狀態資訊，以確定是否顯示「**Trust List Update Failed**」資訊。「**ITL更新失敗**」消息表明電話處於鎖定或不可信狀態，因為它未能用其當前ITL驗證信任清單，並且未能通過TVS驗證信任清單。

如果導航到**Settings > Status > Status Messages**，則可以從電話本身看到**Trust List Update Failed**消息：



也可以從**狀態消息**在電話網頁中看到**信任清單更新失敗消息，如下所示：**



解決方案 — 批次ITL重置

CUCM版本10.0(1)使用可用於在電話和CUCM伺服器之間重新建立信任的附加金鑰。該新金鑰是ITL恢復金鑰。ITL恢復金鑰是在安裝或升級期間建立的。當主機名更改、DNS更改或其他更改執行時，此恢復金鑰不會更改，這些更改可能會導致電話進入不再信任其配置檔案的簽名者的狀態。

當電話處於出現**Trust List Update Failed**消息的狀態時，可以使用新的**utils itl reset** CLI命令在電話或電話與CUCM上的TFTP服務之間重新建立信任。**utils itl reset**命令：

1. 從發佈方節點獲取當前ITL檔案，剝離ITL檔案的簽名，並使用ITL恢復私鑰再次對ITL檔案的內容進行簽名。
2. 自動將新的ITL檔案複製到集群中所有活動的TFTP節點上的TFTP目錄中。
3. 在運行TFTP的每個節點上自動重新啟動TFTP服務。

然後，管理員必須重置所有電話。重置導致電話在從TFTP伺服器啟動時請求ITL檔案，並且電話接收的ITL檔案使用ITLRecovery金鑰而不是**callmanager.pem私鑰**簽名。運行ITL重置有兩種選項：**utils itl reset localkey**和**utils reset remotekey**。ITL重置命令只能從發佈方運行。如果您從訂戶發出ITL重置，則會出現**This is not a Publisher Node**消息。下一節將詳細介紹每個命令的示例。

使用本地恢復金鑰的ITLRecovery

localkey選項使用Publisher硬碟驅動器上的ITLRecovery.p12檔案所包含的ITL Recovery私鑰作為新的ITL檔案簽名者。

```
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
```

帶有遠端恢復金鑰的ITLRecovery

remotekey選項允許指定要儲存ITLRecovery.p12檔案的外部SFTP伺服器。

```
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
```

附註：如果使用remotekey選項完成ITL重置，則發佈器上的localkey（磁碟檔案）將替換為remotekey。

使用「show itl」命令檢驗當前簽名者

如果在發出ITL重置命令之前使用**show itl**命令檢視ITL檔案，則表明ITL包含**ITLRECOVERY_*<publisher_hostname>*條**目。集群中任何TFTP伺服器所服務的每個ITL檔案都包含來自發佈方的此ITL恢復條目。在本示例中，**show itl**命令的輸出來自發佈者。用於簽署ITL的令牌以粗體表示：

```
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.
```

驗證是否使用了ITLRecovery金鑰

如果在執行ITL重置後使用**show itl**命令檢視ITL檔案，則會顯示ITLRecovery條目已簽署ITL，如下所示。在TFTP重新啟動之前，ITLRecovery仍是ITL的簽名者，此時使用**callmanager.pem**或TFTP證書重新對ITL進行簽名。

```
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.
```

增強功能，降低電話失去信任的可能性

除了ITL重置功能之外，CUCM 10.0(1)版還包括管理員功能，幫助防止電話進入不可信狀態。電話具有的兩個信任點是TVS證書(**TVS.pem**)和TFTP證書(**callmanager.pem**)。 在僅有一個CUCM伺服器的最簡單環境中，如果管理員依次重新生成**callmanager.pem**證書和**TVS.pem**證書，電話將重置，並在啟動時顯示**Trust List Update Failed**消息。即使由於重新生成的ITL中包含的證書而從CUCM傳送到電話的自動裝置重置，電話也可以進入不信任CUCM的狀態。

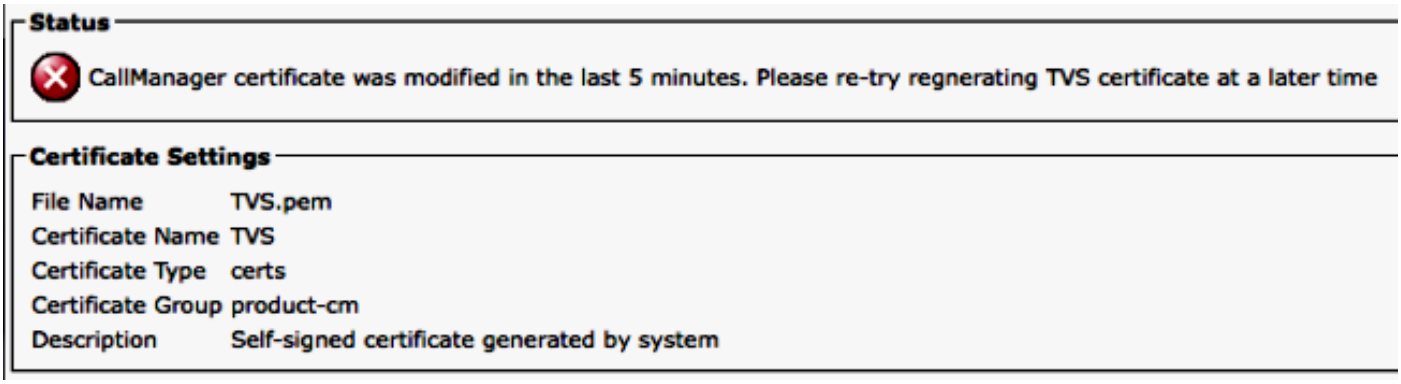
為了幫助防止同時重新生成多個證書（通常是更改主機名或DNS域名修改）的情況，CUCM現在有一個保持計時器。重新生成證書時，CUCM會阻止管理員在上一次證書重新生成的五分鐘內在同一節點上重新生成另一個證書。此過程將導致電話在重新生成第一個證書時重置，並且應在重新生成下一個證書之前備份並註冊。

無論先生成哪個證書，電話都有其驗證檔案的輔助方法。有關此過程的更多詳細資訊，請參閱通訊管理器預設安全和ITL運行與故障排除。

此輸出顯示了以下情況：如從CLI檢視，CUCM阻止管理員在上一次證書重新生成的五分鐘內重新生成另一個證書：

```
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
```

在作業系統(OS)管理頁面上可以看到相同的消息，如下所示：



發佈者ITL恢復金鑰是整個集群使用的唯一金鑰，即使每個節點都有其自己的ITLRecovery證書頒發給**ITLRecovery_*<node name>的公用名(***CN)。發佈者ITLRecovery金鑰是整個集群的ITL檔案中唯一使用的金鑰，如**show itl**命令所示。這就是為什麼ITL文**件中所*見的唯一***ITLRecovery_<hostname>條目包含發佈者的主機名。

如果發佈者的主機名發生更改，ITL中的ITLRecovery條目將繼續顯示發佈者的舊主機名。這是有意造成的，因為ITLRecovery檔案永遠不應更改以確保電話始終信任ITL恢復。

這也適用於域名被更改的情況；在ITLRecovery條目中看到原始域名，以確保恢復金鑰不會更改。ITLRecovery證書的唯一更改時間是證書因有效期為五年而到期並必須重新生成。

可以使用CLI或OS Administration頁面重新生成ITL恢復金鑰對。在發佈者或任何訂閱者上重新生成ITLRecovery證書時，不會重置IP電話。重新生成ITLRecovery證書後，TFTP服務重新啟動，ITL檔案才會更新。在發佈伺服器上重新生成ITLRecovery證書後，請在群集中運行TFTP服務的每個節點上重新啟動TFTP服務，以便使用新證書更新ITL檔案中的ITLRecovery條目。最後一步是從**System > Enterprise Parameters**重置所有裝置，並使用重置按鈕使所有裝置下載包含新ITRecovery證書的新ITL檔案。

備份國際交易日誌恢復

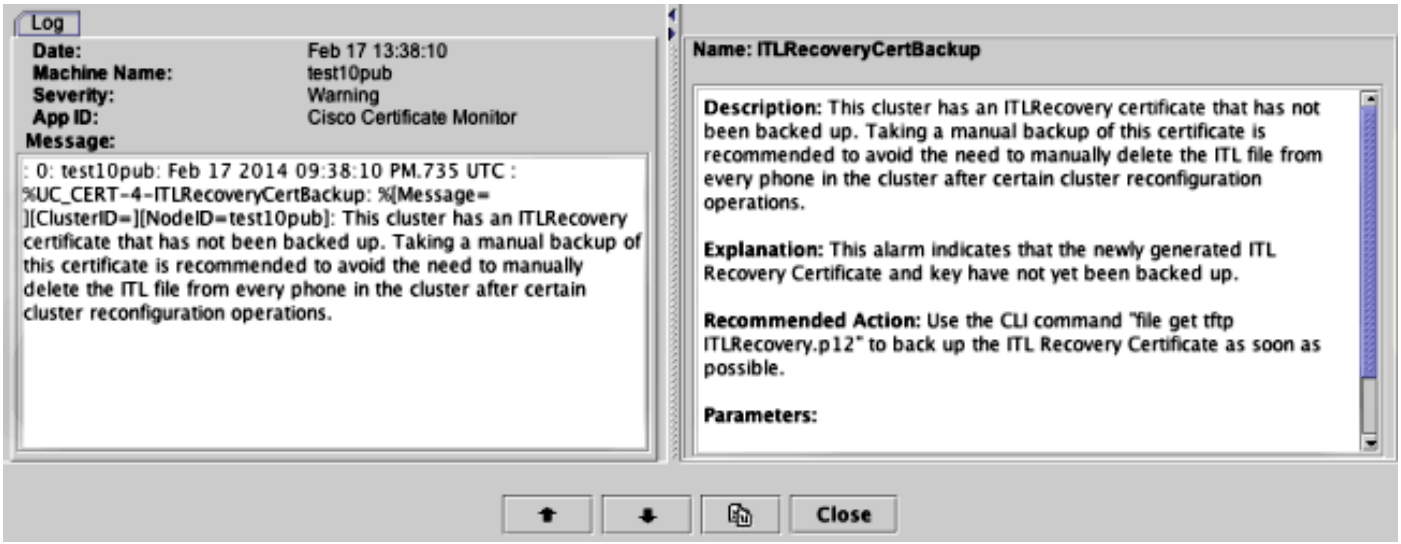
當電話進入不可信狀態時，需要使用ITL恢復金鑰。因此，在備份ITL恢復金鑰之前，每天都會生成新的即時監控工具(RTMT)警報。災難恢復系統(DRS)備份不足以停止警報。儘管建議備份以儲存ITL恢復金鑰，但還需要手動備份金鑰檔案。

要備份恢復金鑰，請登入到發佈伺服器的CLI並輸入**file get tftp ITLRecovery.p12**命令。若要將檔案儲存到，需使用SFTP伺服器，如下圖所示。訂閱伺服器節點沒有ITL恢復檔案，因此如果您在訂閱伺服器上發出**file get tftp ITLRecovery.p12**命令，將導致找不**到檔案**。

```
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
```

從CLI執行手動備份以備份ITLRecovery.p12檔案之前，CiscoSyslog（事件檢視器 — 應用程式日誌）中每天都會顯示一條警告，如下所示。如果從OS Administration頁面**Security > Certificate Monitor**啟用電子郵件通知，則在執行手動備份之前，還可能會收到每日電子郵件。



當DRS備份包含ITLRecovery時，建議仍將ITLRecovery.p12檔案儲存在一個安全的位置，以防備份檔案丟失或損壞，或者選擇重置ITL檔案而無需從備份中恢復。如果儲存了發佈器的ITLRecovery.p12檔案，則它還允許在不備份的情況下重建發佈器，使用DRS還原選項從訂閱者還原資料庫，並通過使用**utils itl reset remotekey**選項重置ITL在電話和CUCM伺服器之間重建信任。

請記住，如果重新生成發佈伺服器，則群集安全密碼應與獲取ITLRecovery.p12檔案的發佈伺服器相同，因為ITLRecovery.p12檔案使用基於群集安全密碼的密碼進行密碼保護。因此，如果更改了群集安全密碼，表示尚未備份ITLRecovery.p12檔案的RTMT警報將重置並每天觸發，直到使用**get tftp ITLRecovery.p12**檔案儲存新的ITLRecovery.p12檔案為止。

驗證

批次國際交易日誌重置功能只有在電話安裝了包含ITLRecovery條目的國際交易日誌時才有效。為了驗證電話上安裝的ITL檔案是否包含ITLRecovery條目，請在每個TFTP伺服器上的CLI中輸入**show itl**命令，以查詢ITL檔案的校驗和。**show itl**命令的輸出顯示校驗和：

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

每個TFTP伺服器上的校驗和不同，因為每台伺服器在其ITL檔案中都有自己的**callmanager.pem**證書。如果您在**Settings > Security Configuration > Trust List**下檢視電話本身的ITL，則可以從電話網頁或從運行較新韌體的電話報告的DeviceTLInfo警報中找到電話上安裝的ITL的校驗和。

大多數運行韌體版本9.4(1)或更高版本的電話使用DeviceTLInfo警報將其ITL的SHA1雜湊報告給CUCM。電話傳送的資訊可以在RTMT的事件檢視器 — 應用日誌中檢視，並與電話使用的TFTP伺

服器ITL雜湊的SHA1雜湊進行比較，以查詢未安裝當前ITL的任何電話，其中包含ITLRecovery條目。

注意事項

- CSCun18578 - ITL重置localkey/remotekey在某些情況下失敗
- CSCun19112 - SFTP錯誤身份驗證型別中的ITL重置遠端金鑰錯誤