Unified Communications Manager バージョン 10.0(1) における ITL の機能拡張

内容

概要

このドキュメントでは、Cisco Unified IP Phone のアイデンティティ信頼リスト（ITL）ファイルの一括リセットを有効にする、Cisco Unified Communications Manager（CUCM）バージョン 10.0(1) の新機能について説明します。ITL 一括リセット機能は、電話が ITL ファイル署名者を信用しなくなり、かつ TFTP サービスからローカルで提供される ITL ファイルを、Trust Verification Service（TVS）を使用して認証できない場合に使用されます。

背景

ITLファイルを一括リセットする機能により、IP PhoneとCUCMサーバ間の信頼を再確立するために、次の手順の1つまたは複数を実行する必要がなくなります。

- 電話機が信頼する古いITLファイルをアップロードするには、バックアップから復元します
- 別のTFTPサーバを使用するように電話機を変更します
- 設定メニューを使用して、電話機からITLファイルを手動で削除します
- ITLを消去するためにアクセスが無効になるように、イベント設定で電話機を出荷時にリセットします

この機能は、電話機をクラスタ間で移動するためのものではありません。この作業を行うには、「CUCM 8およびITLファイルを使用したクラスタ間でのIP Phoneの移行」で説明されている方法のいずれかを使用します。ITLのリセット操作は、IP電話とCUCMクラスタ間の信頼を再確立するために使用され、信頼ポイントが失われた場合にのみ使用されます。

CUCMバージョン10.0(1)で使用できるもう1つのセキュリティ関連機能は、このドキュメントでは説明しませんが、トークンレス証明書信頼リスト(CTL)です。 トークンレスCTLは、ハードウェアUSBセキュリティトークンを、CUCMサーバおよびエンドポイントで暗号化を有効にするために使用されるソフトウェアトークンに置き換えます。詳細については、『IP Phone Security and CTL (Certificate Trust List)』を参照してください。

ITLファイルとセキュリティの詳細については、『Communications Manager Security By Default and ITL Operation and Troubleshooting』を参照してください。

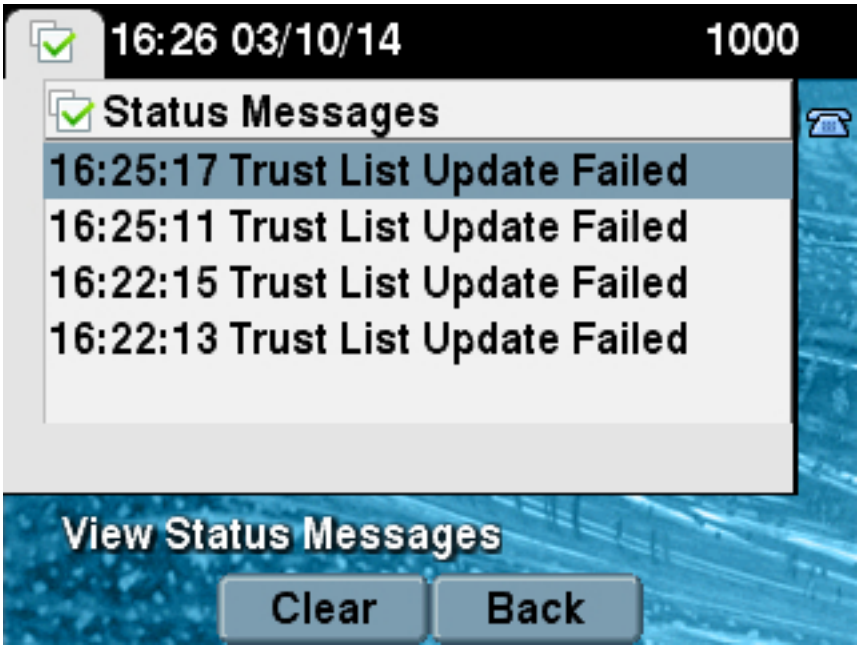
問題の症状

電話機がロックまたは信頼できない状態にある場合は、TFTPサービスによって提供されるITLファイルまたはTFTP設定は受け付けられません。TFTP設定ファイルに含まれている設定変更は、電話機には適用されません。TFTPコンフィギュレーションファイルに含まれる設定の例を次に示します。

- 設定アクセス
- Webアクセス
- セキュアシェル(SSH)アクセス
- スイッチドポートアナライザ(SPAN)からPCポート

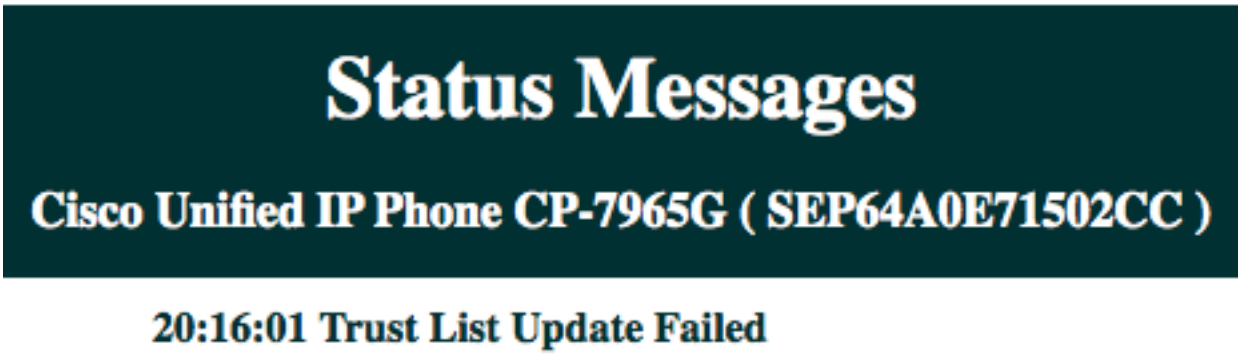
CCM Adminページでこれらの設定のいずれかを電話機に対して変更し、電話機のリセット後に変更が有効にならない場合、電話機がTFTPサーバを信頼しない可能性があります。もう1つの一般的な症状は、社内ディレクトリやその他の電話サービスにアクセスすると、「**Host Not Found**」というメッセージが表示されることです。電話機がロックまたは信頼できない状態であることを確認するには、電話機または電話機のWebページから電話ステータスメッセージを確認し、**[Trust List Update Failed]メッセージが表示されるかどうかを確認します。ITL Update Failed**メッセージは、電話機が現在のITLで信頼リストの認証に失敗し、TVSで認証できなかったため、電話機がロックまたは信頼できない状態であることを示します。

[Settings] > **[Status]** > [**Status** Messages]に移動すると、電話機自体から[Trust List Update Failed]メッセージが**表示されます**。



信頼リスト**の更新に失敗**したメッセージは、次に示すように、電話のWebページのステータスメ

ッセージからも確認できます。



解決策：ITLの一括リセット

CUCMバージョン10.0(1)は、電話機とCUCMサーバ間の信頼を再確立するために使用できる追加キーを使用します。この新しいキーはITLリカバリキーです。ITLリカバリキーは、インストールまたはアップグレード中に作成されます。このリカバリキーは、ホスト名の変更、DNSの変更、またはその他の変更を行っても変更されません。この変更は、電話機が設定ファイルの署名者を信頼しなくなるような状態になる可能性があります。

新しいutils itl reset CLIコマンドを使用して、電話機がTrust List Update Failedメッセージが表示された状態のときに、電話機または電話機とCUCMのTFTPサービスとの間の信頼を再確立できます。utils itl resetコマンド:

1. パブリッシャノードから現在のITLファイルを取得し、ITLファイルの署名を取り除き、ITL Recovery秘密キーを使用してITLファイルの内容に再度署名します。
2. クラスタ内のすべてのアクティブなTFTPノードのTFTPディレクトリに新しいITLファイルを自動的にコピーします。
3. TFTPが稼働するすべてのノードでTFTPサービスが自動的に再起動されます。

その後、管理者がすべての電話機をリセットする必要があります。このリセットにより、電話機はTFTPサーバからの起動時にITLファイルを要求し、電話機が受信するITLファイルは、callmanager.pem秘密キーではなくITLRecoveryキーによって署名されます。ITLリセットを実行するには、次の2つのオプションがあります。utils itl reset localkeyとutils itl reset remotekeyを選択します。ITL resetコマンドは、パブリッシャからのみ実行できます。サブスクライバからITLリセットを発行すると、「This is not a Publisher Node」というメッセージが表示されます。各コマンドの例については、次のセクションで詳しく説明します。

ローカル回復キーによるITLRecovery

localkeyオプションは、新しいITLファイル署名者として、パブリッシャのハードドライブにあるITLRecovery.p12ファイルに含まれるITL回復の秘密キーを使用します。

```
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
```

リモート回復キーによるITLRecovery

remotekeyオプションを使用すると、ITLRecovery.p12ファイルが保存された外部SFTPサーバを指定できます。

```
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**：remotekeyオプションを使用してITLのリセットを実行すると、パブリッシャのlocalkey（ディスクファイル）がremotekeyに置き換えられます。

「show itl」コマンドによる現在の署名者の確認

ITLリセットコマンドを発行する前に**show itlコマンドを使用してITLファイルを表示する**と、ITLに**ITLRECOVERY_*<publisher_hostname>エントリが含まれていることが示され***ます。クラスタ内の任意のTFTPサーバによって処理されるすべてのITLファイルには、パブリッシャからのこのITLリカバリエントリが含まれます。**show itl**コマンドの出力**は**、この例のパブリッシャから取得したものです。ITLに署名するために使用されるトークンは太字で示されています。

```
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.
```

ITLRecoveryキーが使用されていることの確認

ITLのリセットを実行した後にshow itlコマンドを使用してITLファイルを表示すると、ITLRecoveryエントリが次のようにITLに署名したことが示されます。ITLRecoveryは、TFTPが再起動されるまでITLの署名者のままになります。その時点でcallmanager.pemまたはTFTP証明書が使用され、ITLに再度署名します。

```
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.
```

電話機が信頼を失う可能性を減らす機能拡張

ITLリセット機能に加えて、CUCMバージョン10.0(1)には、電話機が信頼できない状態になるのを防ぐのに役立つ管理者権限が含まれています。電話機に設定されている2つのトラストポイントは、TVS証明書(**TVS.pem**)とTFTP証明書(**callmanager.pem**)です。 1台のCUCMサーバしかない最も単純な環境では、管理者が**callmanager.pem証明書とTVS.pem証明書を次々と再生成する**と、電話機がリセットされ、起動時に「**Trust List Update Failed**」メッセージが表示されます。再生成されたITLに含まれる証明書が原因でCUCMから電話機に自動デバイスリセットが送信された場合でも、電話機はCUCMを信頼しない状態になる可能性があります。

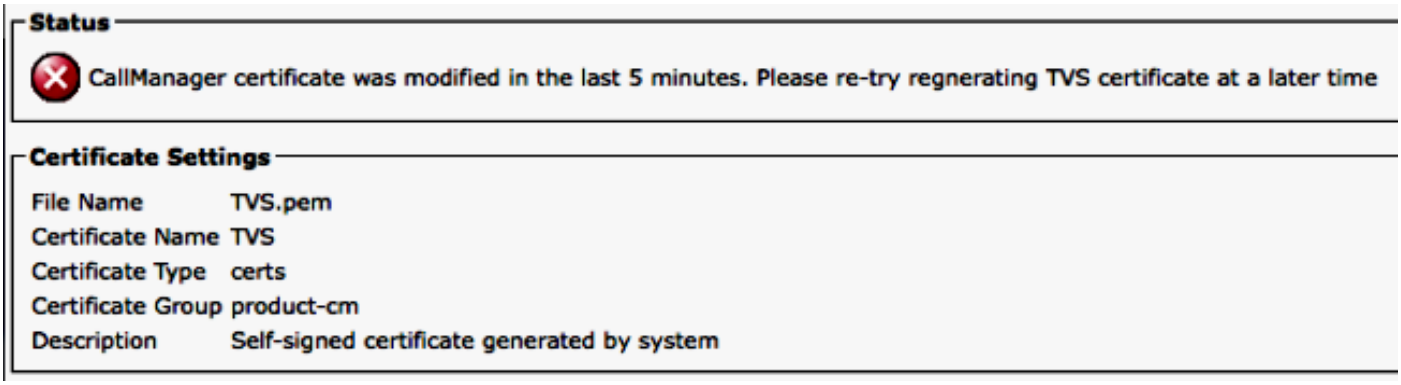
複数の証明書が同時に再生成されるシナリオ（通常はホスト名の変更またはDNSドメイン名の変更）を防ぐために、CUCMにはホールドタイマーが設定されます。証明書が再生成されると、CUCMは、管理者が以前の証明書の再生成から5分以内に同じノード上の別の証明書を再生成しないようにします。このプロセスにより、最初の証明書の再生時に電話機がリセットされ、次の証明書が再生成される前に電話機がバックアップされて登録されます。

どの証明書が最初に生成されるかに関係なく、電話機にはファイルを認証するためのセカンダリメソッドがあります。このプロセスの詳細については、『Communications Manager Security By Default and ITL Operation and Troubleshooting』を参照してください。

次の出力は、CLIから表示して、以前の証明書の再生成から5分以内に管理者が別の証明書を再生成できないようにする状況を示しています。

```
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
```

次に示すように、オペレーティングシステム(OS)の[Administration]ページでも同じメッセージが表示されます。



各ノードが**ITLRecovery_*<node name>の共通名(CN)に発行された独自のITLRecovery証明書を持っていても、クラスタ全体で使用されているパブリッシャのITL回復キーは唯一のキーです。***パブリッシャのITLRecoveryキーは、**show itl**コマンドで表示される、クラスタ全体のITLファイルで使用される唯一のキーで**す。**このため、ITLファイルに**表示される*唯一のITLRecovery_*<hostname>エントリにパブリッシャのホスト名が含まれています。

パブリッシャのホスト名が変更されると、ITLのITLRecoveryエントリにはパブリッシャの古いホスト名が引き続き表示されます。これは、ITLRecoveryファイルを変更して、電話機が常にITL回復を信頼するようにすべきでないためです。

これは、ドメイン名が変更された場合にも適用されます。回復キーが変更されないようにするため、元のドメイン名がITLRecoveryエントリに表示されます。ITLRecovery証明書が変更される唯一の時間は、5年間の有効性が原因で期限切れになり、再生成する必要がある場合です。

ITLリカバリキーペアは、CLIまたはOS管理ページで再生成できます。パブリッシャまたはサブスクライバでITLRecovery証明書が再生成されても、IP Phoneはリセットされません。ITLRecovery証明書が再生成されると、TFTPサービスが再起動されるまで、ITLファイルは更新されません。パブリッシャでITLRecovery証明書を再生成した後、クラスタ内のTFTPサービスを実行するすべてのノードでTFTPサービスを再起動し、ITLファイル内のITLRecoveryエントリを新しい証明書で更新します。最後のステップは、**[System] > [Enterprise Parameters]**からすべてのデバイスをリセットし、リセットボタンを使用して、すべてのデバイスに新しいITLRecovery証

明書を含む新しいITLファイルをダウンロードさせることです。

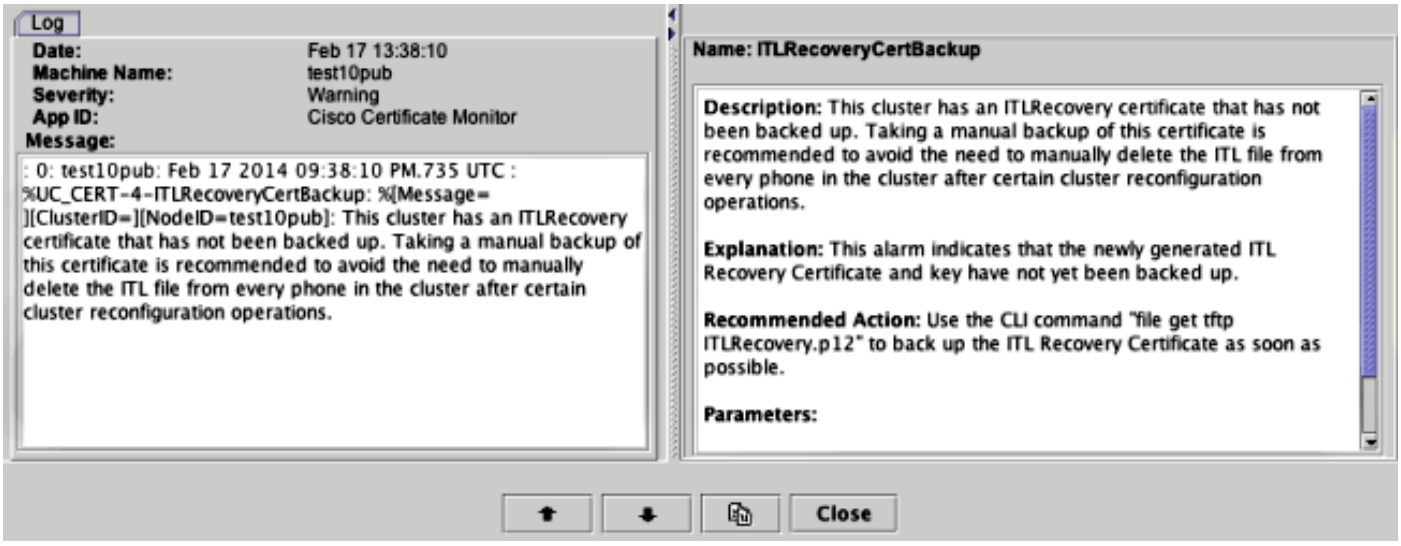
ITLリカバリのバックアップ

ITL回復キーは、電話機が信頼できない状態になったときに回復するために必要です。このため、新しいReal-Time Monitoring Tool(RTMT)アラートは、ITL Recoveryキーがバックアップされるまで毎日生成されます。ディザスタリカバリシステム(DRS)バックアップでは、アラートを停止できません。ITLリカバリキーを保存するにはバックアップを推奨しますが、キーファイルの手動バックアップも必要です。

回復キーをバックアップするには、パブリッシャのCLIにログインし、**file get tftp ITLRecovery.p12コマンドを入力します**。次に示すように、ファイルを保存するにはSFTPサーバが必要です。サブスクライバノードにはITLリカバリファイルがないため、サブスクライバで**file get tftp ITLRecovery.p12コマンドを発行する**と、ファイルが見つかりませ**んでした**。

```
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
```

ITLRecovery.p12ファイルをバックアップするためにCLIから手動バックアップが実行されるまで、次に示すようにCiscoSyslog（イベントビューア – アプリケーションログ）に警告が毎日出力されます。[OS Administration]ページの[**Security**] > [**Certificate Monitor**]で電子メール通知が有効になっている場合、手動バックアップが実行されるまで、毎日の電子メールが受信される場合があります。



DRSバックアップにITLRecoveryが含まれている場合でも、バックアップファイルが失われたり破損した場合に備えてITLRecovery.p12ファイルを安全な場所に保存しておくことをお勧めします。バックアップから復元する必要はありません。パブリッシャからのITLRecovery.p12ファイルが保存されている場合は、**utils itl reset remotekeyオプションを使用してITLをリセットし、DRS復元オプションを使用してバックアップなしでパブリッシャを再構築し、電話機とCUCMサーバ間の間の信頼を再確立します。**

パブリッシャが再構築される場合、クラスタセキュリティパスワードはITLRecovery.p12ファイルの取得元のパブリッシャと同じにする必要があります。これは、ITLRecovery.p12ファイルがクラスタセキュリティパスワードに基づいてパスワードで保護されているためです。このため、クラスタセキュリティパスワードが変更された場合、ITLRecovery.p12ファイルがバックアップされていないことを示すRTMTアラートがリセットされ、**file get tftp ITLRecovery.p12コマンドで新しいITLRecovery.p12ファイルが保存2されるまで毎日トリガーされ**します。

確認

一括ITLリセット機能は、電話機にITLRecoveryエントリを含むITLがインストールされている場合にのみ機能します。電話機にインストールされたITLファイルにITLRecoveryエントリが含まれていることを確認するには、各TFTPサーバのCLIから**show itlコマンドを入力**し、ITLファイルのチェックサムを調べます。**show itl**コマンドの出力に**は、チェックサム**が表示されます。

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

各サーバのITLファイルには独自の**callmanager.pem証明書が含まれているため**、チェックサムはTFTPサーバごとに異なります。電話機にインストールされたITLのITLチェックサムは、電話機のWebページの**[Settings] > [Security Configuration] > [Trust List]でITLを確認するか、新しいファームウェアを実行している電話機から報告されたDeviceTLInfoアラームでを確認できます。**

ファームウェアバージョン9.4(1)以降を実行するほとんどの電話機では、DeviceTLInfoアラームを使用して、ITLのSHA1ハッシュがCUCMに報告されます。電話から送信された情報は、RTMTのEvent Viewer - Application Logで表示できます。また、ITLRecoveryエントリを含む現在のITLがインストールされていない電話を検索するために電話が使用するTFTPサーバのITLハッシュととを比較します。

警告

- CSCun18578:ITL reset localkey/remotekey fails in特定のシナリオ
- CSCun19112:SFTP bad authentication typeのITL reset remotekey error