Менеджер унифицированной связи усовершенствования ITL в версии 10.0 (1)

Содержание

Введение

Этот документ описывает новую характеристику в Версии 10.0 (1) Cisco Unified Communications Manager (CUCM), которая включает объемный сброс файлов Идентификационного списка доверия (ITL) на унифицированных IP-телефонах Cisco. Когда телефоны больше не доверяют подписывающему лицу файла ITL и также не могут аутентифицировать файл ITL, предоставленный Сервисом TFTP локально или с использованием службы проверки доверия (TVS), объемная функция сброса ITL использована.

Общие сведения

Способность увеличить объем сброса файлы ITL предотвращает потребность выполнить один или несколько из этих шагов для восстановления доверия между IP-телефонами и серверами CUCM.

- Восстановление от резервной копии для загрузки старого файла ITL что доверие телефонов
- Измените телефоны для использования другого сервера TFTP
- Удалите файл ITL из телефона вручную через меню Settings
- Фабрика перезагрузила телефон в конечном счете параметры настройки так, чтобы доступ был отключен для стирания ITL

Эта функция не предназначена для перемещения телефонов между кластерами; для той задачи используйте один из методов, описанных в Мигрирующих IP-телефонах Между Кластерами с CUCM 8 и Файлами ITL. Операция сброса ITL используется только для восстановления доверия между IP-телефонами и кластером CUCM, когда они потеряли свои трастовые точки.

Другой связанной с безопасностью функцией, доступной в Версии 10.0 (1) CUCM, которая не покрыта этим документом, является Список доверия Certficate (CTL) Tokenless. CTL Tokenless заменяет аппаратные маркеры безопасности USB программным маркером, используемым для включения шифрование на серверах CUCM и оконечных точках. Для дополнительных сведений обратитесь к Безопасности IP-телефона и CTL (Список надежных сертификатов) документ.

Дополнительные сведения о файлах ITL и безопасности по умолчанию могут быть найдены в диспетчере связи Секурити по умолчанию и Операцией ITL и Документацией по устранению проблем.

Признаки проблемы

Когда телефоны находятся в **блокированном** или **ненадежном состоянии**, они не принимают файл ITL или конфигурацию TFTP, предоставленную Сервисом TFTP. Любое изменение конфигурации, которое содержится в файле конфигурации TFTP, не применено к телефону. Некоторые примеры параметров настройки, которые содержатся в файле конфигурации TFTP:

- Доступ параметров настройки
- Веб - доступ
- Доступ Secure Shell (SSH)
- Коммутируемый анализатор для портов (SPAN) к порту ПК

Если какая-либо из этих настроек изменена для телефона на Странице администратора CCM и, после того, как телефон перезагружен, изменения не вступают в силу, телефон не мог бы доверять серверу TFTP. Другой распространенный симптом - при доступе к корпоративному каталогу или другим телефонным службам, **Хост** сообщения **Не Найденные** показы. Чтобы проверить, что телефон находится в блокированном или ненадежном состоянии, проверьте сообщения состояния телефона с самого телефона или телефонной веб-страницы, чтобы видеть, отображается ли **Трастовое Сообщение об ошибках Обновления Списка**. **Сообщение об ошибках Обновления ITL** является индикатором, что телефон находится в блокированном или ненадежном состоянии, потому что это было не в состоянии аутентифицировать трастовый список со своим текущим ITL и было не в состоянии аутентифицировать его с TVS.

Если вы перешли к **Settings> Status> Status Messages, Трастовое Сообщение об ошибках Обновления Списка** может быть замечено по самому телефону:

Трастовое Сообщение об ошибках Обновления Списка может также быть замечено по телефонной веб-странице из **Сообщений о статусе** как показано здесь:

Решение - увеличивает объем сброса ITL

Версия 10.0 (1) CUCM использует дополнительный ключ, который может использоваться для восстановления доверия между телефонами и серверами CUCM. Этот новый ключ является ключом Восстановления ITL. Ключ Восстановления ITL создан во время установки или обновления. Этот ключ восстановления не изменяется, когда имя хоста изменяется, изменения DNS, или другие изменения выполнены, который мог бы привести к проблемам, где телефоны входят в состояние, где они больше не доверяют подписывающему лицу своих файлов конфигурации.

Новый **utils itl** команда CLI **сброса** может использоваться для восстановления доверия между телефоном или телефонами и Сервисом TFTP на CUCM, когда телефоны находятся в состоянии, где замечено **Трастовое Сообщение об ошибках Обновления Списка**. **Utils itl команда reset**:

1. Берет текущий файл ITL от узла издателя, лишает подпись файла ITL и подписывает содержание файла ITL снова с секретным ключом Восстановления ITL.
2. Автоматически копирует новый файл ITL к каталогам TFTP на всех активных узлах TFTP в кластере.
3. Автоматически перезапускает Сервисы TFTP на каждом узле, куда выполняется TFTP.

Администратор должен тогда перезагрузить все телефоны. Сброс заставляет телефоны запрашивать, чтобы файл ITL на загрузился от сервера TFTP и файла ITL, который получает телефон, подписан ключом ITLRecovery вместо **callmanager.pem** секретного ключа. Существует две опции для выполнения сброса ITL: **utils itl перезагружают localkey**, и **utils itl перезагружают remotekey**. Команда reset ITL может только быть выполнена от издателя. При запуске сброса ITL от абонента он приводит к **Этому, не** сообщение **Узла Издателя**. Примеры каждой команды детализированы в следующих разделах.

ITLRecovery с локальным ключом восстановления

localkey опция использует секретный ключ Восстановления ITL, содержавшийся в подарке файла ITLRecovery.p12 на жестком диске Издателя как подписывающее лицо нового файла 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 с удаленным ключом восстановления

remotekey опция позволяет внешний сервер SFTP, от которого файл ITLRecovery.p12 был сохранен, чтобы быть заданным.

```
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
```

> **Примечание:** Если сброс ITL сделан с remotekey опцией, localkey (на файле на диске) на издателе заменен remotekey.

Проверьте Текущее Подписывающее лицо с Командой "покажите itl"

При просмотре файла ITL с **командой show itl** перед запуском команды reset ITL это показывает, что ITL содержит **ITLRECOVERY _ *<publisher_hostname>*** запись. Каждый файл ITL, который подается любым сервером TFTP в кластере, содержит эту запись восстановления ITL от издателя. Выходные данные **команды show itl** взяты от издателя в данном примере. Маркер, используемый для подписания ITL, полужирным:

```
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.
```

Проверьте, что Используется Ключ ITLRecovery

При просмотре файла ITL с **командой show itl** после выполнения сброса ITL это показывает, что запись ITLRecovery подписала ITL как показано здесь. ITLRecovery остается подписывающим лицом ITL, пока TFTP не перезапущен, в котором времени сертификат **callmanager.pem** или TFTP используется для подписания ITL снова.

```
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.
```

Усовершенствования для уменьшения возможности телефонов, теряющих доверие

В дополнение к возможности сброса ITL Версия 10.0 (1) CUCM включает функции администратора, что справка препятствует тому, чтобы телефоны ввели ненадежное состояние. Два доверия указывает, телефон имеет, сертификат TVS **(TVS.pem)** и сертификат TFTP **(callmanager.pem)**. В самой простой среде только с одним сервером CUCM, если администратор восстанавливает **callmanager.pem** сертификат и сертификат **TVS.pem** одно право за другим, телефонный сброс и на загрузку отображает **Трастовое Сообщение об ошибках Обновления Списка**. Даже со сбросом автоматического устройства, передаваемым с CUCM на телефон из-за сертификата, содержавшегося в ITL, который восстановлен, телефон может ввести состояние, где это не доверяет CUCM.

Чтобы помочь предотвращать сценарий, где несколько серверов сертификатов восстановлены в то же время (как правило, изменение имени хоста или модификации названия Домена DNS), CUCM теперь имеет таймер ожидания. Когда сертификат восстановлен, CUCM препятствует тому, чтобы администратор восстановил другой сертификат на том же узле в течение пяти минут после предыдущей регенерации сертификата. Этот процесс заставляет телефоны быть перезагруженными после регенерации первого сертификата, и они должны быть резервным копированием и зарегистрированный, прежде чем будет восстановлен следующий сертификат.

Независимо от которого сертификат генерируется сначала, телефон имеет свой вторичный метод для аутентификации файлов. Дополнительные сведения об этом процессе могут быть найдены в диспетчере связи Секурити по умолчанию и Операцией ITL и Устранением проблем.

Эти выходные данные показывают ситуацию, где CUCM препятствует тому, чтобы администратор восстановил другой сертификат в течение пяти минут после предыдущей регенерации сертификата, как просматривается от 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
```

То же сообщение может быть замечено по Странице администратора операционной системы (OS) как показано здесь:

Ключ восстановления ITL издателя является единственным в использовании всем кластером, даже при том, что каждый узел имеет свой собственный сертификат ИТЛРЕКОВЕРИ, выполненный к Общему имени (CN) **ИТЛРЕКОВЕРИ _ *<имя узла>***. Ключ издателя Итлрековери является единственным, используемым в файлах ITL для всего кластера, как замечено по **команде show itl**. Это - то, почему единственный **ИТЛРЕКОВЕРИ _** запись ***<hostname>***, замеченная в файле ITL, содержит имя хоста издателя.

Если имя хоста издателя изменено, запись ITLRecovery в ITL продолжает показывать старое имя хоста издателя. Это сделано преднамеренно, потому что файл ITLRecovery никогда не должен изменяться, чтобы гарантировать, что телефоны всегда доверяют восстановлению ITL.

Когда доменные имена изменены также, это просит; исходное имя домена замечено в записи ITLRecovery, чтобы гарантировать, что не изменяется ключ восстановления. Единственное время, которое должен изменить сертификат ITLRecovery, - когда это истекает из-за пятилетней законности и должно быть восстановлено.

Пары ключей восстановления ITL могут быть восстановлены или с CLI или со Страницей администрирования операционной системы. Когда сертификат ITLRecovery восстановлен на издателе или любом из абонентов, IP-телефоны не перезагружены. Как только сертификат ITLRecovery был восстановлен, файл ITL не обновляет, пока Сервис TFTP не перезапущен. После регенерации сертификата ITLRecovery на издателе перезапустите Сервис TFTP на каждом узле, который выполняет Сервис TFTP в кластере для обновления записи ITLRecovery в файле ITL с новым сертификатом. Заключительный шаг должен перезагрузить все устройства от **Системы> Параметры предприятия** и использовать кнопку сброса, чтобы заставить все устройства загрузить новый файл ITL, который содержит новый сертификат ITLRecovery.

Резервное копирование восстановление ITL

Ключ Восстановления ITL требуется для восстановления телефонов, когда они вводят ненадежное состояние. Из-за этого, новые предупреждения устройства контроля в реальном времени (RTMT) ежедневно генерируются, пока ключ Восстановления ITL не выполнен резервное копирование. Резервная копия системы аварийного восстановления (DRS) не достаточна для остановки предупреждений. Несмотря на то, что резервная копия рекомендуется для сохранения ключа Восстановления ITL, ручная резервная копия контрольного файла необходима также.

Для выполнения резервное копирование ключа восстановления войдите к CLI издателя и войдите**, файл получают** команду **ITLRecovery.p12 tftp**. Сервер SFTP необходим, чтобы

сохранить файл к как показано здесь. Узлы абонента не имеют файла восстановления ITL, поэтому если вы выходите**, файл получают** команду **ITLRecovery.p12 tftp** на абоненте, это приводит к **файлу, не найденному**.

```
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
```

Пока ручная резервная копия не выполнена от CLI для выполнения резервное копирование файла ITLRecovery.p12, предупреждение распечатано в CiscoSyslog (Просмотр событий - Журнал приложения) каждый день как показано здесь. Ежедневное электронное письмо могло бы также быть получено, пока ручная резервная копия не выполнена, если почтовое уведомление включено от Страницы администрирования операционной системы, **Безопасность> Монитор Сертификата**.

В то время как резервная копия DRS содержит ITLRecovery, рекомендуется все еще хранить файл ITLRecovery.p12 в безопасном расположении в случае, если резервные файлы потеряны или повреждены или для имения опции для сброса файла ITL без потребности восстановить от резервной копии. Если у вас есть файл ITLRecovery.p12 от сохраненного издателя, он также позволяет издателю быть восстановленным без резервной копии с использованием, опция восстановления DRS, чтобы восстановить базу данных от susbcriber и восстановить доверие между телефонами и серверами CUCM путем сброса ITL с **utils itl перезагрузила remotekey** опцию.

Помните, что, если издатель восстановлен, кластерный надежный пароль должен совпасть с издателем, где файл ITLRecovery.p12 был взят от того, потому что файл ITLRecovery.p12 защищен паролем с паролем, основанным прочь кластерного надежного пароля. Поэтому, если кластерный надежный пароль изменен, предупреждение RTMT, которое указывает, файл ITLRecovery.p12 не был выполнен резервное копирование, перезагружен и ежедневно инициирует, пока новый файл ITLRecovery.p12 не сохранен с **файлом, получают** команду **ITLRecovery.p12 tftp**.

Проверка

Объемные ITL перезагружают функцию, только работает, если телефонам установили ITL, который содержит запись ITLRecovery. Чтобы проверить, что файл ITL, установленный по телефонам, содержит запись ITLRecovery, введите **команду show itl** от CLI на каждом из серверов TFTP для обнаружения контрольной суммы файла ITL. Выходные данные от

команды show itl отображают контрольную сумму:

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

Контрольная сумма является другой на каждом сервере TFTP, потому что каждый сервер имеет свой собственный **callmanager.pem** сертификат в его файле ITL. Контрольная сумма ITL ITL, установленного по телефону, может быть найдена, просматриваете ли вы ITL по самому телефону в соответствии с**> Security Параметров настройки Конфигурация>, Трастовый Список**, от телефонной веб-страницы, или от сигнала тревоги DeviceTLInfo сообщил по телефонам, что выполняет более новое микропрограммное обеспечение.

Большинство телефонов, которые выполняют версию микропрограммы 9.4 (1) или более поздний отчёт хэш SHA1 их ITL к CUCM с сигналом тревоги DeviceTLInfo. Информация, передаваемая телефоном, может быть просмотрена в конечном счете Средство просмотра - Журнал приложения от RTMT и по сравнению с хэшем SHA1 хэша ITL серверов TFTP использование телефонов для обнаружения любых телефонов, которым не установили текущий ITL, который содержит запись ITLRecovery.

Предупреждения

- CSCun18578 - ITL перезагружают сбои localkey/remotekey в определенных сценариях
- CSCun19112 - ITL перезагружают remotekey ошибку в типе неправильной проверки подлинности SFTP