Miglioramenti ITL di Unified Communications Manager nella versione 10.0(1)

Sommario

Introduzione

Questo documento descrive una nuova funzionalità di Cisco Unified Communications Manager (CUCM) versione 10.0(1) che consente la reimpostazione di massa dei file ITL (Identity Trust List) sui telefoni IP unificati Cisco. La funzione di reimpostazione ITL in blocco viene utilizzata quando i telefoni non considerano più attendibile il firmatario del file ITL e non possono inoltre autenticare il file ITL fornito dal servizio TFTP in locale o con l'utilizzo del servizio di verifica dell'attendibilità (TVS).

Sfondo

La possibilità di reimpostare in blocco i file ITL evita di dover eseguire uno o molti di questi passaggi per ristabilire la fiducia tra i telefoni IP e i server CUCM.

- Ripristinare da un backup per caricare un vecchio file ITL considerato attendibile dai telefoni
- Cambiare i telefoni per utilizzare un server TFTP diverso
- Elimina manualmente il file ITL dal telefono tramite il menu delle impostazioni
- Il telefono è stato reimpostato nelle impostazioni dell'evento in modo che l'accesso sia disabilitato per cancellare l'ITL

Questa funzionalità non è progettata per spostare i telefoni tra cluster. per questa operazione, utilizzare uno dei metodi descritti in Migrazione di telefoni IP tra cluster con file CUCM 8 e ITL. L'operazione di reimpostazione ITL viene utilizzata solo per ristabilire il trust tra i telefoni IP e il cluster CUCM quando questi hanno perso i propri trust point.

Un'altra funzionalità relativa alla sicurezza disponibile in CUCM versione 10.0(1) non illustrata in questo documento è l'elenco di certificati attendibili senza token (CTL). Il CTL senza token sostituisce i token di sicurezza USB dell'hardware con un token software utilizzato per abilitare la crittografia sui server e sugli endpoint CUCM. Per ulteriori informazioni, fare riferimento al documento IP Phone Security and CTL (Certificate Trust List).

Per ulteriori informazioni sui file ITL e sulla protezione per impostazione predefinita, vedere il documento Sicurezza predefinita di Communications Manager e Operazione ITL e risoluzione dei problemi.

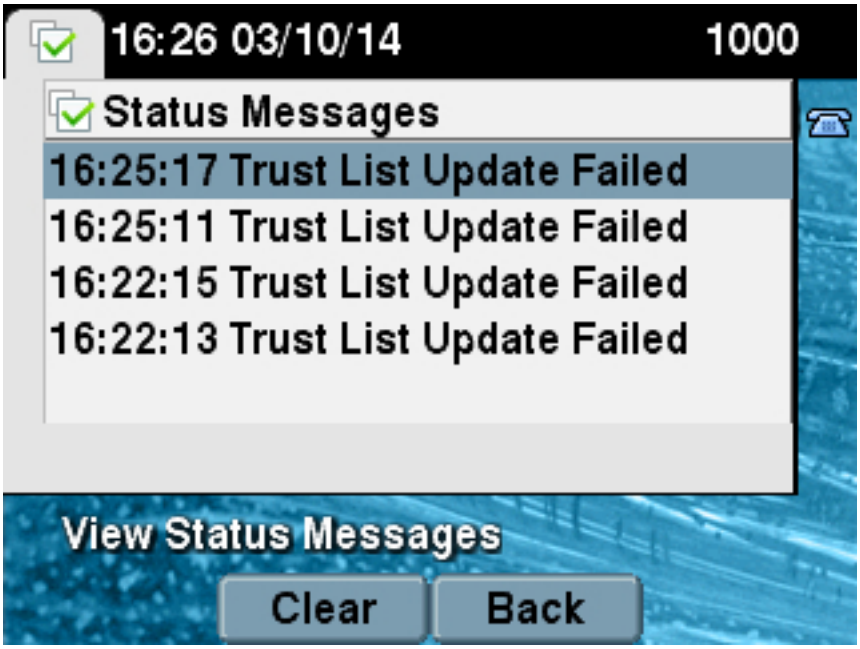
Sintomi dei problemi

Quando i telefoni sono in stato **bloccato** o **non attendibile**, non accettano il file ITL o la configurazione TFTP forniti dal servizio TFTP. Le modifiche alla configurazione contenute nel file di configurazione TFTP non vengono applicate al telefono. Di seguito sono riportati alcuni esempi di impostazioni contenute nel file di configurazione TFTP:

- Accesso alle impostazioni
- Accesso Web
- Accesso Secure Shell (SSH)
- SPAN (Switched Port Analyzer) su porta PC

Se una qualsiasi di queste impostazioni viene modificata per un telefono nella pagina Amministrazione CCM e, dopo la reimpostazione del telefono, le modifiche non hanno effetto, il telefono potrebbe non considerare attendibile il server TFTP. Un altro sintomo comune è rappresentato dal messaggio **Host non trovato** visualizzato quando si accede all'elenco in linea aziendale o ad altri servizi telefonici. Per verificare che lo stato del telefono sia bloccato o non attendibile, controllare i messaggi di stato del telefono inviati dal telefono stesso o dalla pagina Web del telefono per verificare se viene visualizzato un messaggio di **aggiornamento dell'elenco di attendibilità non riuscito**. Il messaggio **Aggiornamento ITL non riuscito** indica che il telefono è in uno stato bloccato o non attendibile perché non è riuscito ad autenticare l'elenco di trust con l'ITL corrente e non è riuscito ad autenticarlo con la TV.

Il messaggio **Aggiornamento elenco di attendibilità non riuscito** può essere visualizzato dal telefono stesso se si seleziona **Impostazioni > Stato > Messaggi di stato**:



Il messaggio **Aggiornamento elenco di attendibilità non riuscito** può essere visualizzato anche dalla pagina Web del telefono dai **messaggi di stato** come mostrato di seguito:

Soluzione - Reset ITL in blocco

CUCM versione 10.0(1) utilizza una chiave aggiuntiva che può essere utilizzata per ristabilire la fiducia tra i telefoni e i server CUCM. Questa nuova chiave è la chiave di ripristino ITL. La chiave di ripristino ITL viene creata durante l'installazione o l'aggiornamento. Questa chiave di ripristino non viene modificata quando vengono apportate modifiche al nome host, al DNS o ad altre modifiche che potrebbero causare problemi quando i telefoni passano in uno stato in cui non considerano più attendibile il firmatario dei file di configurazione.

Il nuovo comando **utils itl reset** CLI può essere usato per ristabilire la fiducia tra uno o più telefoni e il servizio TFTP su CUCM quando i telefoni si trovano in uno stato in cui viene visualizzato il messaggio **Trust List Update Failed** (**Aggiornamento elenco trust non riuscito)**. Il comando **utils itl reset**:

1. Prende il file ITL corrente dal nodo dell'editore, rimuove la firma del file ITL e firma di nuovo il contenuto del file ITL con la chiave privata ITL Recovery.
2. Copia automaticamente il nuovo file ITL nelle directory TFTP su tutti i nodi TFTP attivi nel cluster.
3. Riavvia automaticamente i servizi TFTP su ogni nodo in cui viene eseguito il protocollo TFTP.

L'amministratore deve quindi ripristinare tutti i telefoni. Il reset fa sì che i telefoni richiedano il file ITL all'avvio dal server TFTP e che il file ITL ricevuto dal telefono sia firmato dalla chiave ITLRecovery invece che dalla chiave privata **callmanager.pem**. Per eseguire un ripristino ITL, è possibile procedere in due modi: **utils itl reset localkey** e **utils itl reset remotekey**. Il comando di reimpostazione ITL può essere eseguito solo dal server di pubblicazione. Se si esegue una reimpostazione ITL da un sottoscrittore, viene visualizzato il messaggio **Questo non è un nodo del server di pubblicazione**. Nelle sezioni seguenti vengono illustrati alcuni esempi di ciascun comando.

ITLRecovery con la chiave di ripristino locale

L'opzione localkey utilizza la chiave privata ITL Recovery contenuta nel file ITLRecovery.p12 presente sul disco rigido del server di pubblicazione come nuovo firmatario del file 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 con la chiave di ripristino da remoto

L'opzione remotekey consente di specificare il server SFTP esterno da cui è stato salvato il file ITLRecovery.p12.

```
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
```

> **Nota:** Se viene eseguita una reimpostazione ITL con l'opzione remotekey, la chiave locale (nel file su disco) dell'autore viene sostituita con la chiave remota.

Verificare il firmatario corrente con il comando "show itl"

Se si visualizza il file ITL con il comando **show itl** prima di eseguire un comando ITL reset, il file ITL conterrà una voce **ITLRECOVERY_*<publisher_hostname>***. Ogni file ITL fornito da un server TFTP nel cluster contiene questa voce di recupero ITL dal server di pubblicazione. In questo esempio, l'output del comando **show itl** viene generato dall'autore. Il token usato per firmare l'ITL è in grassetto:

```
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.
```

Verificare che sia utilizzata la chiave ITLRecovery

Se si visualizza il file ITL con il comando **show itl** dopo aver eseguito una reimpostazione ITL, la voce ITLRecovery ha firmato l'ITL come mostrato di seguito. ITLRecovery rimane il firmatario dell'ITL fino al riavvio del TFTP, momento in cui viene utilizzato il certificato **callmanager.pem** o TFTP per firmare di nuovo l'ITL.

```
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.
```

Miglioramenti per diminuire la possibilità di perdita di fiducia dei telefoni

Oltre alla funzionalità di ripristino ITL, CUCM versione 10.0(1) include funzioni di amministrazione che impediscono ai telefoni di entrare in uno stato non attendibile. I due trust point del telefono sono il certificato TVS (**TVS.pem**) e il certificato TFTP (**callmanager.pem**). Nell'ambiente più semplice con un solo server CUCM, se un amministratore rigenera il certificato **callmanager.pem** e il certificato **TVS.pem** uno dopo l'altro, il telefono si reimposta e all'avvio viene visualizzato il messaggio **Aggiornamento elenco di attendibilità non riuscito**. Anche con un ripristino automatico del dispositivo inviato da CUCM al telefono a causa di un certificato contenuto nell'ITL rigenerato, il telefono può entrare in uno stato in cui non considera attendibile CUCM.

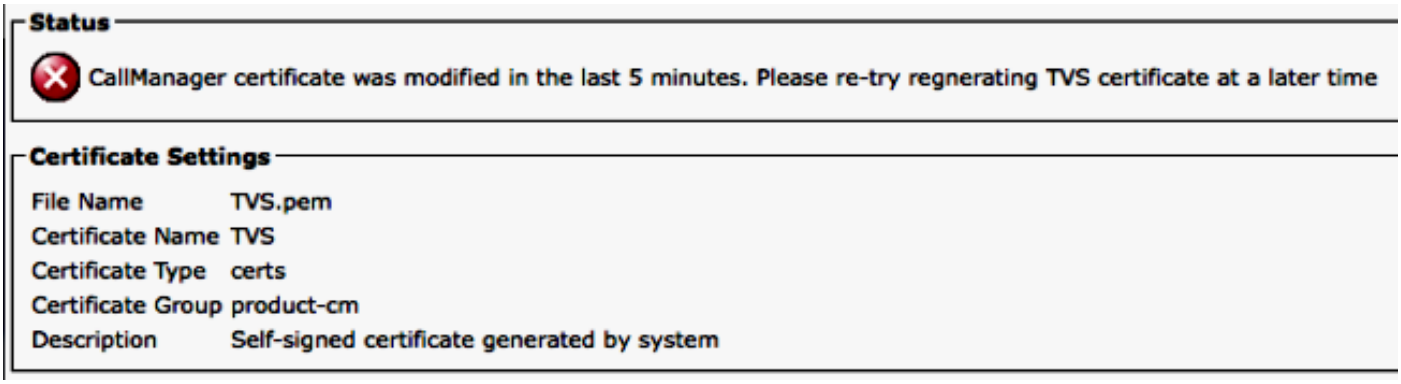
Per evitare che vengano rigenerati più certificati contemporaneamente, in genere la modifica del nome host o il cambiamento del nome di dominio DNS, CUCM dispone ora di un timer di attesa. Quando un certificato viene rigenerato, CUCM impedisce all'amministratore di rigenerare un altro certificato sullo stesso nodo entro cinque minuti dalla precedente rigenerazione del certificato. Questo processo determina il reset dei telefoni durante la rigenerazione del primo certificato. È necessario eseguire il backup e la registrazione dei telefoni prima della rigenerazione del certificato successivo.

Indipendentemente dal certificato generato per primo, il telefono ha il suo metodo secondario per autenticare i file. Per ulteriori informazioni su questo processo, vedere Sicurezza predefinita di Communications Manager e Operazioni e risoluzione dei problemi ITL.

Questo output mostra una situazione in cui CUCM impedisce all'amministratore di rigenerare un altro certificato entro cinque minuti dalla precedente rigenerazione del certificato visualizzata dalla 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
```

Lo stesso messaggio può essere visualizzato dalla pagina Amministrazione del sistema operativo (OS) come mostrato di seguito:



La chiave di ripristino ITL del server di pubblicazione è l'unica utilizzata dall'intero cluster, anche se ogni nodo dispone di un proprio certificato ITLRecovery rilasciato al Nome comune (CN) di **ITLRecovery_*<node name>***. La chiave ITLRecovery del server di pubblicazione è l'unica utilizzata nei file ITL per l'intero cluster come indicato dal comando **show itl**. Ecco perché l'unica **voce ITLRecovery_*<hostname>*** presente in un file ITL contiene il nome host dell'autore.

Se il nome host dell'autore viene modificato, la voce ITLRecovery nell'ITL continua a indicare il nome host precedente dell'autore. Questo è fatto intenzionalmente perché il file ITLRecovery non dovrebbe mai cambiare per garantire che i telefoni sempre considerano attendibile il recupero ITL.

Ciò vale anche quando vengono modificati i nomi di dominio. il nome di dominio originale viene visualizzato nella voce ITLRecovery per garantire che la chiave di ripristino non cambi. L'unica volta in cui il certificato ITLRecovery deve essere modificato è quando scade a causa della validità di cinque anni e deve essere rigenerato.

Le coppie di chiavi di ripristino ITL possono essere rigenerate dalla CLI o dalla pagina Amministrazione del sistema operativo. I telefoni IP non vengono reimpostati quando il certificato ITLRecovery viene rigenerato nel server di pubblicazione o in uno dei sottoscrittori. Dopo la rigenerazione del certificato ITLRecovery, il file ITL non viene aggiornato fino al riavvio del servizio TFTP. Dopo la rigenerazione del certificato ITLRecovery nel server di pubblicazione, riavviare il servizio TFTP in ogni nodo che esegue il servizio TFTP nel cluster per aggiornare la voce ITLRecovery nel file ITL con il nuovo certificato. Il passaggio finale consiste nel ripristinare tutti i dispositivi da **Sistema > Parametri Enterprise** e utilizzare il pulsante di ripristino per fare in modo che tutti i dispositivi scarichino il nuovo file ITL che contiene il nuovo certificato ITLRecovery.

Eseguire il backup del ripristino ITL

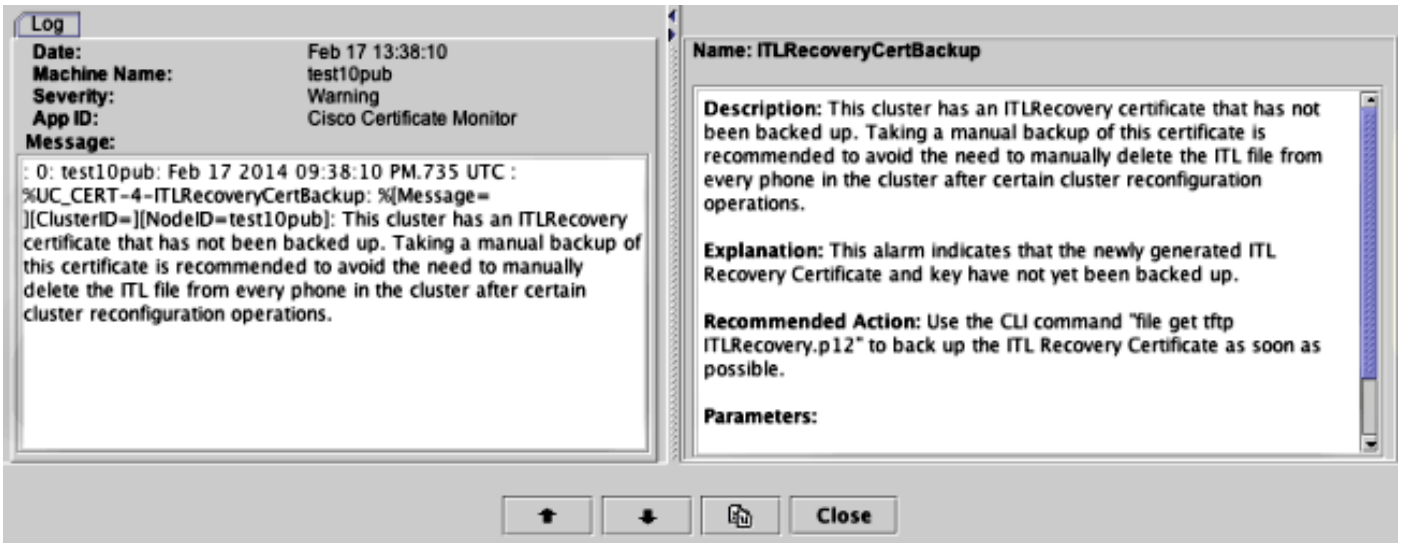
La chiave di ripristino ITL è necessaria per ripristinare i telefoni in stato non attendibile. Per questo motivo, vengono generati quotidianamente nuovi avvisi tramite Real-Time Monitoring Tool (RTMT) fino a quando non viene eseguito il backup della chiave ITL Recovery. Un backup del Disaster Recovery System (DRS) non è sufficiente per interrompere gli allarmi. Sebbene sia consigliato un backup per salvare la chiave di ripristino ITL, è necessario anche un backup manuale del file di chiave.

Per eseguire il backup della chiave di ripristino, accedere alla CLI dell'autore e immettere il comando **get tftp ITLRecovery.p12**. Per salvare il file in è necessario un server SFTP, come mostrato di seguito. I nodi del sottoscrittore non dispongono di un file di recupero ITL, quindi se si esegue il comando **file get tftp ITLRecovery.p12** su un sottoscrittore, il **file non** verrà **trovato**.

```
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
```

Finché non viene eseguito il backup manuale dalla CLI per eseguire il backup del file ITLRecovery.p12, ogni giorno viene stampato un avviso in CiscoSyslog (Visualizzatore eventi - Registro applicazioni), come mostrato di seguito. È inoltre possibile ricevere un messaggio e-mail giornaliero fino a quando non viene eseguito il backup manuale se la notifica e-mail è abilitata dalla pagina Amministrazione del sistema operativo, **Protezione > Monitoraggio certificati**.



Mentre un backup DRS contiene ITLRecovery, si consiglia di conservare il file ITLRecovery.p12 in un luogo sicuro in caso di perdita o danneggiamento dei file di backup o per avere la possibilità di ripristinare il file ITL senza dover eseguire il ripristino da un backup. Se il file ITLRecovery.p12 dell'editore è stato salvato, consente anche di ricostruire l'editore senza un backup con l'opzione di ripristino DRS per ripristinare il database da un sottoscrittore e ristabilire la fiducia tra i telefoni e i server CUCM reimpostando l'ITL con l'opzione **utils itl reset remotekey**.

Tenere presente che se il server di pubblicazione viene ricostruito, la password di protezione del cluster deve essere la stessa del server di pubblicazione da cui è stato prelevato il file ITLRecovery.p12, in quanto il file ITLRecovery.p12 è protetto da password con una password basata sulla password di protezione del cluster. Per questo motivo, se la password di protezione del cluster viene modificata, l'avviso RTMT che indica che il file ITLRecovery.p12 non è stato sottoposto a backup viene reimpostato e viene attivato ogni giorno finché il nuovo file ITLRecovery.p12 non viene salvato con il comando **file get tftp ITLRecovery.p12**.

Verifica

La funzione di ripristino ITL in blocco funziona solo se sui telefoni è installato un ITL che contiene la voce ITLRecovery. Per verificare che il file ITL installato sui telefoni contenga la voce ITLRecovery, immettere il comando **show itl** dalla CLI su ciascuno dei server TFTP per trovare il checksum del file ITL. L'output del comando **show itl** visualizza il checksum:

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

Il checksum è diverso su ogni server TFTP in quanto ogni server dispone del proprio certificato **callmanager.pem** nel proprio file ITL. Il checksum ITL dell'ITL installato sul telefono può essere trovato se si visualizza l'ITL sul telefono stesso in **Impostazioni > Configurazione di sicurezza > Elenco di attendibilità**, dalla pagina Web del telefono o dall'allarme DeviceTLInfo segnalato dai telefoni che eseguono firmware più recente.

La maggior parte dei telefoni con firmware versione 9.4(1) o successive segnala l'hash SHA1 del proprio ITL a CUCM con l'allarme DeviceTLInfo. Le informazioni inviate dal telefono possono essere visualizzate nel Visualizzatore eventi - Registro applicazioni da RTMT e confrontate con l'hash SHA1 dell'hash ITL dei server TFTP utilizzati dai telefoni per trovare qualsiasi telefono che non abbia l'attuale ITL installato, che contiene la voce ITLRecovery.

Avvertenze

- CSCun18578 - La reimpostazione della chiave locale/chiave remota ITL non riesce in alcuni scenari
- CSCun19112 - Errore di reimpostazione della chiave remota ITL in un tipo di autenticazione non valido SFTP