Verbeteringen in Unified Communications Manager ITL, versie 10.0(1)

Inhoud

Inleiding

Dit document beschrijft een nieuwe functie in Cisco Unified Communications Manager (CUCM) versie 10.0(1), waarmee de bulkreset van Identity Trust List (ITL) bestanden op Cisco Unified IP-telefoons kan worden uitgevoerd. De functie voor het terugstellen van de bulksite ITL wordt gebruikt wanneer telefoons niet langer vertrouwen hebben in de ITL-bestandsinteur en het ITL-bestand niet lokaal of met het gebruik van de TVS (Trust Verification Service) kunnen authenticeren.

Achtergrond

De mogelijkheid om ITL-bestanden in bulk te resetten voorkomt de noodzaak om een of veel van deze stappen uit te voeren om het vertrouwen tussen IP-telefoons en de CUCM-servers te herstellen.

- Een back-up herstellen om een oud ITL-bestand te uploaden dat de telefoons vertrouwen
- Verander de telefoons om een andere TFTP server te gebruiken
- Verwijdert het ITL-bestand handmatig uit de telefoon via het instellingsmenu
- Stel de telefoon in de instellingen van de gebeurtenis opnieuw in zodat de toegang wordt uitgeschakeld om de ITL te wissen

Deze eigenschap is niet bedoeld om telefoons tussen clusters te bewegen; Gebruik voor die taak een van de methoden die zijn beschreven in IP-telefoons migreren tussen clusters met CUCM 8- en ITL-bestanden. De ITL reset-handeling wordt alleen gebruikt om het vertrouwen tussen IP-

telefoons en de CUCM-cluster opnieuw te bevestigen wanneer ze hun trust points hebben verloren.

Een andere security-gerelateerde optie die beschikbaar is in CUCM versie 10.0(1) en die niet in dit document is opgenomen, is de Tokenless Certficate Trust List (CTL). De Tokenless CTL vervangt de hardware-USB security penningen met een softwaretoken die worden gebruikt om encryptie op de CUCM-servers en endpoints mogelijk te maken. Raadpleeg voor meer informatie het IP-telefoon security en CTL-document (certificaatlijst).

Aanvullende informatie over de ITL-bestanden en de standaardinstelling van de beveiliging is te vinden in het document Communications Manager Security by Default en ITL Operatie and Troubleshooter Document.

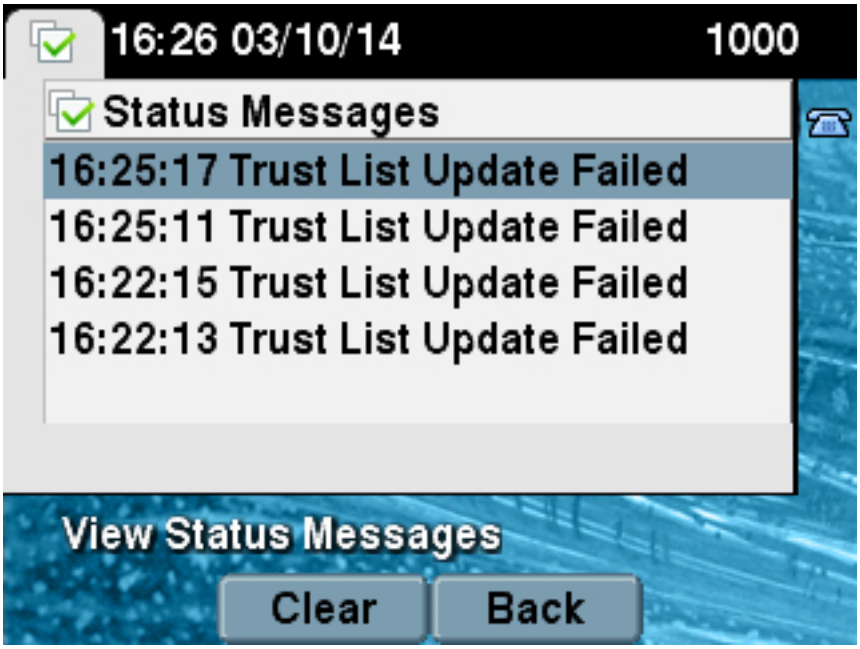
Probleemsymptomen

Wanneer telefoons in een **gesloten** of **onvertrouwde** staat zijn, aanvaarden zij het ITL-bestand of de TFTP-configuratie die door de TFTP-dienst is verstrekt, niet. Elke configuratieverandering die in het TFTP-configuratiebestand zit, is niet van toepassing op de telefoon. Enkele voorbeelden van instellingen die in het TFTP-configuratiebestand zijn opgenomen zijn:

- Instellingen toegang
- Webtoegang
- Secure Shell (SSH)-toegang
- Switched Port Analyzer (SPAN) naar PC-poort

Als een van deze instellingen voor een telefoon op de CCM Admin pagina wordt gewijzigd en, nadat de telefoon wordt gereset, worden de veranderingen niet van kracht, kan de telefoon de TFTP server niet vertrouwen. Een ander algemeen symptoom is wanneer u tot de bedrijvenfolder of andere telefoondiensten toegang hebt, het bericht **Host Not Found** displays. Om te verifiëren dat de telefoon in een gesloten of onvertrouwde staat is, controleer de berichten van de telefoonstatus van de telefoon zelf of de telefoon webpagina om te zien of een **Update van de Lijst van het Vertrouwen mislukt** bericht. Het bericht voor **bijwerken** ITL mislukt is een indicator dat de telefoon in een vergrendelde of onvertrouwde staat is geplaatst omdat het de vertrouwenslijst niet echt heeft gemaakt met het huidige ITL en niet heeft geauthentiseerd met TVS.

Het bericht **Update** van de **Lijst van het Vertrouwen** kan van de telefoon zelf worden gezien als u naar **Instellingen > Status > Statusberichten** navigeert:



Het bericht **Update** van de **Lijst van het Vertrouwen** kan ook van de telefoon van de **Statusberichten** zien zoals hier getoond wordt:

Oplossing - bulk ITL-reset

CUCM versie 10.0(1) gebruikt een extra sleutel die kan worden gebruikt om het vertrouwen tussen telefoons en de CUCM-servers te herstellen. Deze nieuwe toets is de ITL-toets voor herstel. De ITL-hersteltoets wordt tijdens de installatie of upgrade gemaakt. Deze terugwinningssleutel verandert niet wanneer de hostname verandert, DNS verandert, of andere veranderingen worden uitgevoerd die kunnen leiden tot problemen waar de telefoons in een staat komen waar zij niet langer de ontwerper van hun configuratiebestanden vertrouwen.

De nieuwe **utils it reset** CLI-opdracht kan worden gebruikt om het vertrouwen tussen een telefoon of telefoons en de TFTP-service op CUCM te herstellen wanneer de telefoons in een toestand zijn waarin het bericht Lijst met **failliet van** de **vertrouwenslijst** wordt weergegeven. De **optie Deze wordt opnieuw ingesteld**:

1. Neemt het huidige ITL-bestand van het uitgeverij-knooppunt, verwijdert de handtekening van het ITL-bestand en tekent opnieuw de inhoud van het ITL-bestand met de privé-toets voor ITL-herstel.
2. Kopieert automatisch het nieuwe ITL-bestand naar de TFTP-directories op alle actieve TFTP-knooppunten in het cluster.
3. Start automatisch de TFTP-services op elk knooppunt waar TFTP draait.

De beheerder moet dan alle telefoons resetten. De reset veroorzaakt dat de telefoons om het ITL-bestand te vragen bij het opstarten vanaf de TFTP-server en het ITL-bestand dat de telefoon ontvangt, wordt ondertekend door de ITLRectie-toets in plaats van de privétoets **callmanager.pem**. Er zijn twee opties om een ITL-reset uit te voeren: **Hiermee stelt u de lokale toets in** en **stelt u de externe toets in**. De ITL reset-opdracht kan alleen vanuit de uitgever worden uitgevoerd. Als u een ITL-reset uit een abonnee geeft, levert dit **geen** bericht van **Node voor uitgevers op**. In de volgende secties worden voorbeelden van elke opdracht gegeven.

ITLR-herstel met de toets voor lokaal herstel

De localkey optie gebruikt de private ITL-toets voor herstel in het ITLRecrecovery.p12-bestand dat op de vaste schijf van de uitgever aanwezig is als de nieuwe ITL-bestandsextender.

```
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-herstel met de toets voor extern herstel

Met de optie Remote-key kan de externe SFTP-server worden gespecificeerd waarvan het ITLRecedent.p12-bestand is opgeslagen.

```
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
```

> **Opmerking:** Als er een ITL-reset is uitgevoerd met de optie remotekey, dan wordt de localkey (op de disk file) op de uitgever vervangen door de remotekey.

Controleer het huidige gebaar met de opdracht "tonen IT"

Als u het ITL-bestand met de opdracht **tonen** voordat u een ITL-reset-opdracht geeft, toont dit aan dat de ITL een **ITL**-ingang bevat **ITLRECOVERY_*<uitgever_hostname>***. Elk ITL-bestand dat door een TFTP-server in de cluster wordt bediend, bevat deze ITL-terugwinningsingang van de uitgever. De output van de **show itl** opdracht wordt genomen van de uitgever in dit voorbeeld. Het token dat wordt gebruikt voor het tekenen van het ITL is vet:

```
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.
```

Controleer of de ITLR-toets wordt gebruikt

Als u het ITL-bestand met de opdracht **tonen** bekijkt nadat u een ITL-reset hebt uitgevoerd, dan toont dit aan dat de ITL-opname heeft getekend zoals hier wordt weergegeven. Het ITLR-herstel blijft de ontwerper van het ITL totdat het TFTP is hervat, op welk tijdstip het **callmanager.pem** of TFTP-certificaat wordt gebruikt om het ITL opnieuw te ondertekenen.

```
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.

Verbeteringen om de mogelijkheid van telefoons die vertrouwen verliezen te verminderen

Naast de ITL reset mogelijkheid, bevat CUCM versie 10.0(1) beheerfuncties die helpen voorkomen dat telefoons een onvertrouwde status binnengaan. De twee trust points die de telefoon heeft zijn het TVS certificaat (**TVS.pem**) en het TFTP certificaat (**callmanager.pem**). In de eenvoudigste omgeving met slechts één CUCM-server, als een beheerder het **callmanager.pem-**certificaat opnieuw genereert en het **TVS.pem-**certificaat één voor één, wordt de telefoon opnieuw ingesteld en bij Opstartvertraging wordt het bericht voor update van de **vertrouwenslijst** weergegeven. Zelfs met een automatisch apparaat dat van CUCM naar de telefoon wordt verzonden wegens een certificaat in het ITL dat wordt geregenereerd, kan de telefoon een staat binnendringen waar het geen CUCM vertrouwt.

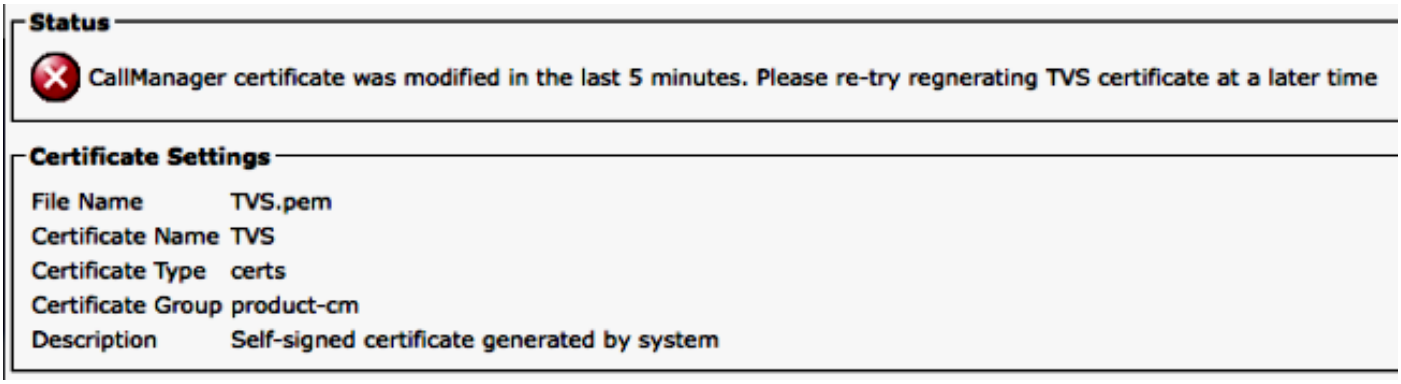
Om het scenario te helpen voorkomen waar meerdere certificaten tegelijkertijd worden gegenereerd (meestal hostname verandering of DNS domeinnaamwijzigingen) heeft CUCM nu een Hold timer. Wanneer een certificaat wordt geregenereerd, voorkomt CUCM dat de beheerder een ander certificaat op hetzelfde knooppunt regenereert binnen vijf minuten na de vorige certificatie-regeneratie. Via dit proces worden de telefoons opnieuw opgestart na het eerste certificaat. Er moet een back-up worden gemaakt en geregistreerd voordat het volgende certificaat opnieuw wordt gegenereerd.

Ongeacht welke certificaat eerst wordt gegenereerd heeft de telefoon zijn secundaire methode om bestanden te authentiseren. Aanvullende informatie over dit proces kan worden gevonden in Unified Communications Manager Security by Default en ITL Operating and Troubleshooter.

Deze uitvoer toont een situatie waarin CUCM verhindert dat de beheerder een ander certificaat regenereert binnen vijf minuten na een vorige regeneratie van het certificaat zoals bekeken vanuit de 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
```

Hetzelfde bericht kan worden gezien op de pagina van het besturingssysteem (Operating System) Administration (OS) zoals hieronder wordt weergegeven:



De uitgeverij ITL-terugwinningssleutel is de enige die door de gehele cluster wordt gebruikt, ook al heeft elk knooppunt een eigen ITLRecedecertificaat dat is afgegeven voor de Gemeenschappelijke Naam (GN) van **ITLRecrecovery_*<knoopnaam>***. De uitgever ITLRecedesleutel is de enige die in de ITL bestanden voor het gehele cluster zoals gezien van de **show itl** opdracht wordt gebruikt. Dit is waarom de enige **ITLRecrecovery_*<hostname>***die in een ITL-bestand is gezien, de hostnaam van de uitgever bevat.

Als de hostname van de uitgever wordt gewijzigd, blijft de ITLRrecuperatie in het ITL de oude hostname van de uitgever tonen. Dit wordt opzettelijk gedaan omdat het ITLR-herstelbestand nooit zou moeten veranderen om er zeker van te zijn dat de telefoons altijd het ITL-herstel vertrouwen.

Dit geldt wanneer ook domeinnamen worden gewijzigd; de oorspronkelijke domeinnaam wordt in het ITLRectopport weergegeven om ervoor te zorgen dat de terugvorderingstoets niet verandert. De enige keer dat het ITLRecertificaat moet worden gewijzigd, is dat het vervalt vanwege de vijfjarige geldigheid en moet worden teruggegeven.

De ITL-terugwinningstoetsenborden kunnen met de CLI- of de OS-beheerpagina worden gegenereerd. IP-telefoons worden niet gereset wanneer het ITLR-certificaat opnieuw op de uitgever of een van de abonnees wordt gegenereerd. Nadat het ITLR-certificaat is hersteld, werkt het ITL-bestand niet bij totdat de TFTP-dienst opnieuw is gestart. Na de regeneratie van het ITLR-certificaat op de uitgever, start de TFTP-dienst opnieuw op elk knooppunt dat de TFTP-dienst in het cluster runt, om de ITLR-recuperatie in het ITL-bestand met het nieuwe certificaat bij te werken. De laatste stap is het terugstellen van alle apparaten van **Systeem > Enterprise parameters** en het gebruiken van de reset knop om alle apparaten het nieuwe ITL-bestand te laten downloaden dat het nieuwe ITL-certificaat bevat.

Terug naar ITL-herstel

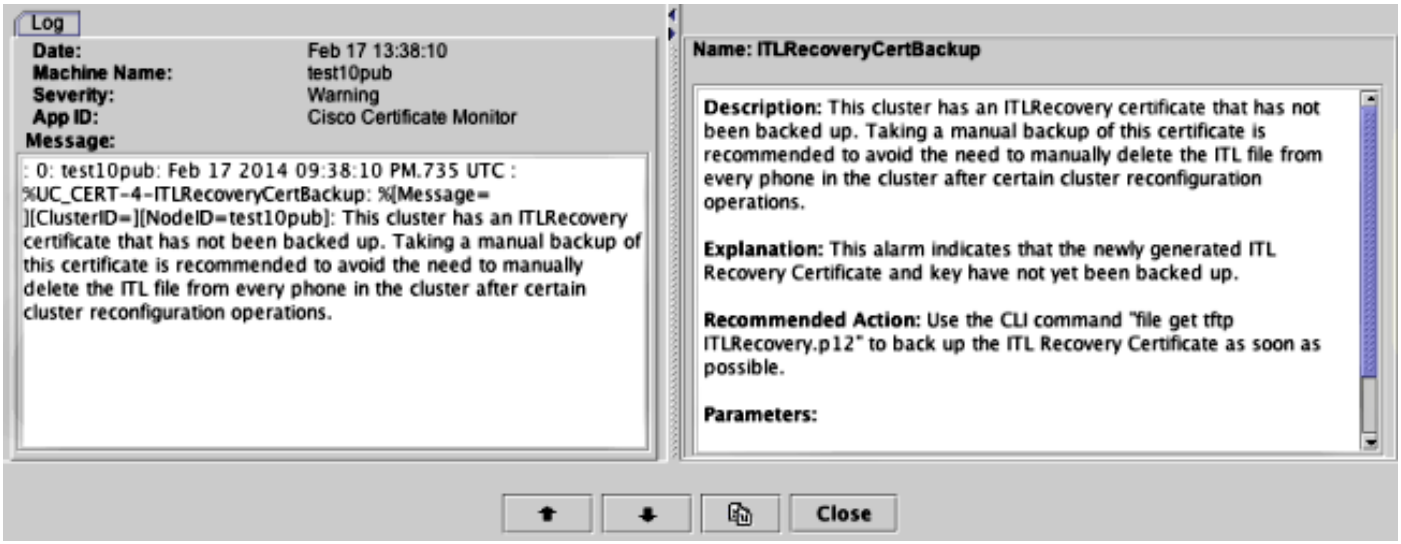
De ITL-toets voor herstel is vereist om telefoons te kunnen herstellen wanneer ze een onvertrouwde status invoeren. Hierdoor worden dagelijks nieuwe RTMT-waarschuwingen (Real-Time Monitoring Tool) gegenereerd totdat van de ITL-toets voor herstel een back-up is gemaakt. Een back-up van het noodherstel systeem (DRS) is niet voldoende om de waarschuwingen te stoppen. Hoewel een back-up wordt aanbevolen om de ITL-toets voor herstel op te slaan, is ook een handmatige back-up van het hoofdbestand nodig.

Om een back-up van de terugwinningssleutel te maken, logt u in bij de CLI van de uitgever en geeft u de opdracht **ITLRecrecovery.p12** in. Er is een SFTP-server nodig om het bestand op te slaan naar zoals hier wordt weergegeven. Subscriber-knooppunten hebben geen ITL-herstelbestand, dus als u het **bestand** geeft en **ITLRectoptie.p12**-opdracht op een abonnee geeft,

levert dit **bestand** op **dat niet gevonden is**.

```
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
```

Totdat de handmatige back-up van de CLI wordt uitgevoerd om back-ups te maken van het ITLRecrecovery.p12-bestand, wordt er elke dag een waarschuwing afgedrukt in CiscoSlug (Event Viewer - Application Log), zoals hier wordt weergegeven. Er kan ook een dagelijkse e-mail worden ontvangen totdat de handmatige back-up wordt uitgevoerd als e-mailkennisgeving is ingeschakeld vanaf de OS-beheerpagina, **Security > certificaatmonitor**.



Terwijl een DRS-back-up de ITLRectoptie bevat, wordt aanbevolen het ITLRecrecovery.p12-bestand nog steeds op een veilige locatie op te slaan, indien de reservekopieën verloren of beschadigd zijn, of om de optie te hebben om het ITL-bestand opnieuw in te stellen zonder dat u uit een back-up hoeft te herstellen. Als u het ITLRecedent.p12-bestand hebt opgeslagen van de uitgever, kan de uitgever ook worden hergebouwd zonder back-up met behulp van de optie DRS om de database van een abonnee te herstellen en het vertrouwen tussen de telefoons en CUCM-servers te herstellen door de ITL opnieuw in te stellen met de optie **util** en **remotekey**.

Denk eraan dat als de uitgever wordt herbouwd, het wachtwoord voor de clusterbeveiliging hetzelfde zou moeten zijn als de uitgever waar het ITLRecrecovery.p12-bestand is afgeleid omdat het ITLRecrecovery.p12-bestand is beveiligd met een wachtwoord dat is gebaseerd op het wachtwoord voor de clusterbeveiliging. Om deze reden, als het wachtwoord voor de

clusterbeveiliging wordt gewijzigd, wordt de RTMT-waarschuwing die aangeeft dat er geen back-up is gemaakt voor het ITLRecrecovery.p12-bestand, dagelijks teruggezet en geactiveerd totdat het nieuwe ITLRecrecovery.p12-bestand is opgeslagen met de opdracht **voor het** bestand **Tftp ITLRecedp.p12**.

Verifiëren

De bulkreset optie van ITL werkt alleen als telefoons een ITL hebben geïnstalleerd die de zoekfunctie voor ITLR bevat. Om te verifiëren dat het ITL-bestand dat op de telefoons is geïnstalleerd de ITLRrecovery-ingang bevat, **voert** u de opdracht **show itl in** van de CLI op elk van de TFTP-servers om de checksum van het ITL-bestand te vinden. De uitvoer van het **bevel van de show** toont de checksum:

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

De checksum is verschillend op elke TFTP-server omdat elke server een eigen **callmanager.pem**-certificaat heeft in zijn ITL-bestand. Het ITL-checksum van het ITL dat aan de telefoon is geïnstalleerd, kan worden gevonden als u het ITL aan de telefoon bekijkt onder **Instellingen > Beveiligingsconfiguratie > Vertrouwenlijst**, van de webpagina van het telefoonnetwerk of van het apparaatTLInfo-alarm dat is gemeld door telefoons die nieuwere firmware uitvoeren.

De meeste telefoons die firmware versie 9.4(1) uitvoeren of rapporteren later de SHA1-hash van hun ITL naar CUCM met het Devices-TLInfo-alarm. De informatie die door de telefoon wordt verstuurd, kan in het Event Viewer - Application Log van RTMT worden bekeken en vergeleken met de SHA1 hash van de ITL hash van de TFTP-servers die de telefoons gebruiken om telefoons te vinden die de huidige ITL niet hebben geïnstalleerd, wat de ITLR-opname bevat.

Caveats

- CSCun18578 - Plaatselijk opnieuw ingesteld/remotekey faalt in bepaalde scenario's
- CSCun19112 - fout bij verwijdering van ITL bij SFTP slecht authenticatietype