Herstel van certificaten voor CUCM

Inhoud

Inleiding

Dit document beschrijft de procedure om certificaten in Cisco Unified Communications Manager (CUCM) release 8.x en hoger te regenereren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- *Realtime bewaking tool* (RTMT)
- CUCM-certificaten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CUCM release 8.X en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document beschrijft de stapsgewijze procedure voor het regenereren van certificaten in Cisco Unified Communications Manager (CUCM) release 8.x en nieuwer. Dit weerspiegelt echter niet de veranderingen na 12.0 in het herstel van ITL.

RTMT installeren

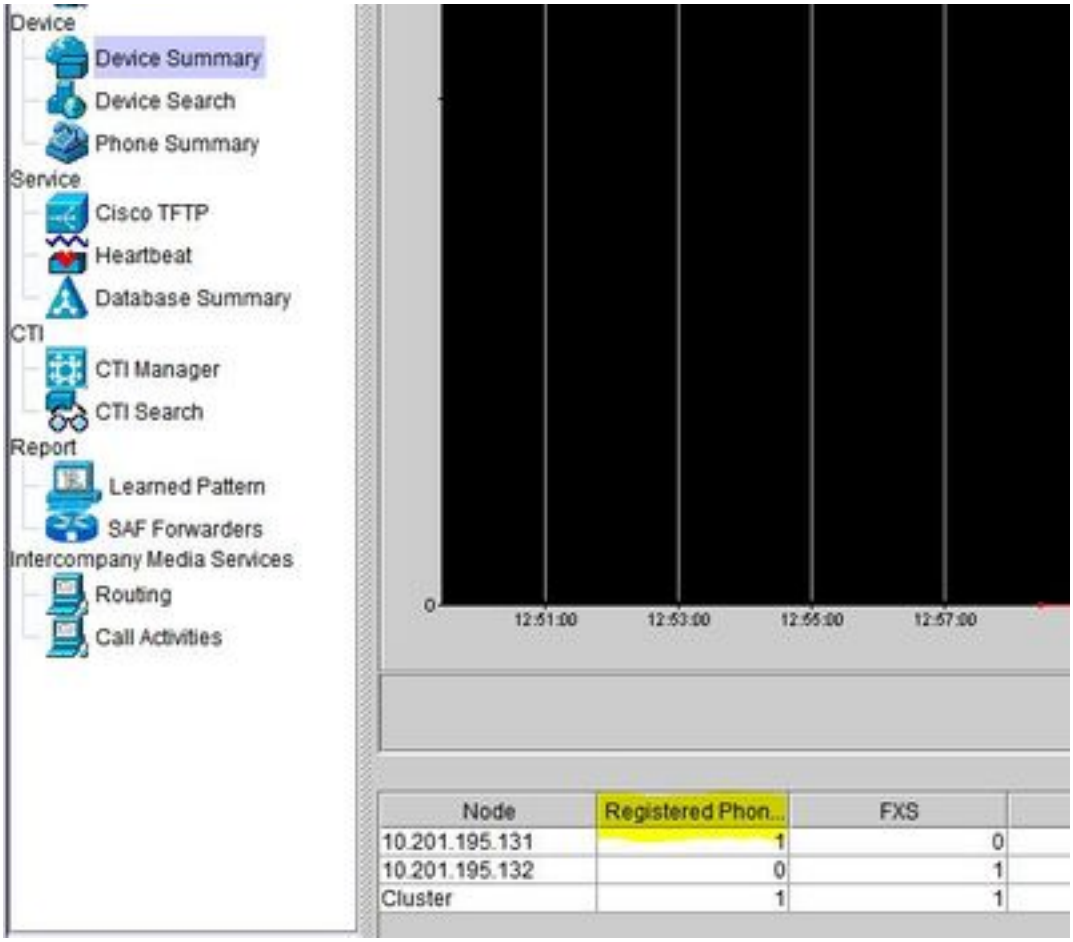
- Download en installeer RTMT Tool van Call Manager. Navigeren naar Call Manager (CM)-beheer: **Toepassing > Plugins > Zoeken > Cisco Unified Real-Time Monitoring Tool - Windows > Downloaden** Installeren en starten

Monitorendpoints met RTMT

- Start RTMT en voer het IP-adres of de volledig gekwalificeerde domeinnaam (FQDN) in, en voer vervolgens de gebruikersnaam en het wachtwoord in om toegang te krijgen tot de tool:
- Selecteer het **tabblad Spraak/video**.Selecteer **Apparaatoverzicht**. In deze sectie wordt het totale aantal geregistreerde eindpunten en het aantal punten per knooppunt aangegevenControleer tijdens het opnieuw instellen van het eindpunt om registratie te garanderen voordat het volgende certificaat wordt vernieuwd

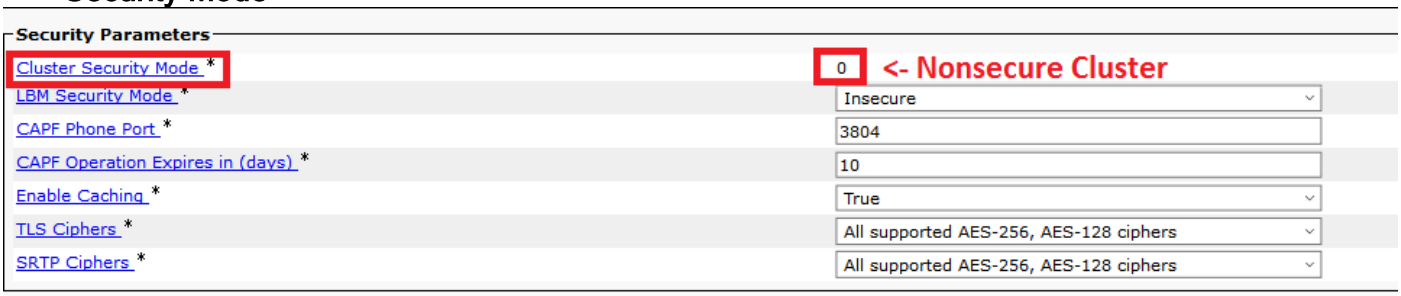
Tip: Het regeneratieproces van sommige certificaten kan invloed hebben op endpoints. Overweeg een actieplan na regelmatige kantooruren toe te schrijven aan het vereiste om de diensten opnieuw te beginnen en telefoons te rebooten. Controleer of registratie via RTMT ten zeerste wordt aanbevolen.

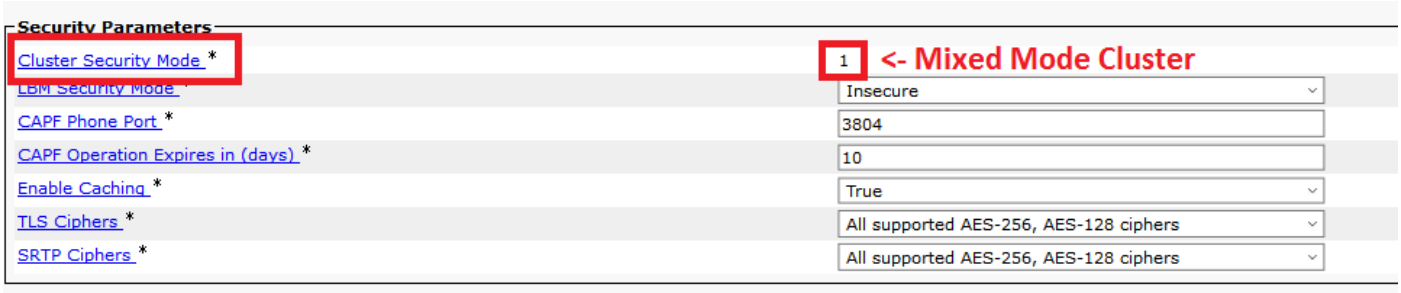
Waarschuwing: Endpoints met huidige ITL-mismatch kunnen na dit proces registratieproblemen hebben. De verwijdering van het ITL op het eindpunt is een typische best practice-oplossing nadat het regeneratieproces is voltooid en alle andere telefoons zijn geregistreerd.



Identificeer als uw cluster in de gemengde of niet-beveiligde modus staat

- Ga naar SCM-beheer. **Systeem > Enterprise Parameters > Beveiligingsparameters > Cluster Security Mode**





Effect door het certificaatarchief

Het is essentieel voor succesvolle systeemfunctionaliteit om alle certificaten over de CUCM-cluster te laten bijwerken. Als certificaten verlopen of ongeldig zijn, kunnen ze de normale functionaliteit van het systeem aanzienlijk beïnvloeden. De gevolgen kunnen afwijken, afhankelijk

van de installatie van uw systeem. Een lijst van diensten voor de specifieke certificaten die ongeldig of verlopen zijn wordt hier getoond:

CallManager.pem

- Versleutelde/geverifieerde telefoons registreren niet
- Trivial File Transfer Protocol (TFTP) is niet vertrouwd (telefoons accepteren geen ondertekende configuratiebestanden en/of ITL-bestanden)
- De telefoondiensten kunnen worden beïnvloed
- Secure Session Initiation Protocol (SIP)-trunks of -media (conferentiebruggen, Media Termination Point (MTP), Xcoders, enzovoort) registreren of werken niet.
- Het AXL-verzoek mislukt.

Tomcat.pem

- Telefoons hebben geen toegang tot HTTP-services die worden gehost op de CUCM-knooppunt, zoals Corporate Directory
- CUCM kan verschillende web problemen, zoals niet kunnen toegang tot service pagina's van andere knooppunten in het cluster
- Extension Mobility (EM) of Extension Mobility Cross Cluster-problemen
- Single Sign-On (SSO)
- Als UCCX (Unified Contact Center Express) is geïntegreerd, moet u vanwege de beveiligingswijzigingen van CCX 12.5 het CUCM Tomcat-certificaat (zelfondertekend) of het Tomcat-wortel- & tussencertificaat (voor CA-ondertekend) in de UCCX tomcat-trust-winkel hebben geüpload, omdat het Finesse-desktoplogins uitvoert.

CAPF.pem

- Telefoons verifiëren niet voor Phone VPN, 802.1x of Phone Proxy
- Kan geen LSC-certificaten (Local Significant Certificate) voor de telefoons uitgeven.
- Versleutelde configuratiebestanden werken niet

IPsec.pem

- Noodherstelsysteem (DRS)/noodherstelkader (DRF) kan niet goed functioneren
- IPsec-tunnels naar gateway (GW) naar andere CUCM-clusters werken niet

TVS (Trust Verification Service)

Trust Verification Service (TVS) is de belangrijkste component van Security by Default. Met TV kunnen Cisco Unified IP-telefoons toepassingsservers, zoals EM-services, directory en MIDlet, verifiëren wanneer HTTPS is ingesteld.

TVS biedt de volgende functies:

- Schaalbaarheid - resources voor Cisco Unified IP-telefoon worden niet beïnvloed door het aantal certificaten dat moet worden vertrouwd.

- Flexibiliteit - Het toevoegen of verwijderen van vertrouwenscertificaten wordt automatisch weerspiegeld in het systeem.
- Beveiliging op standaard - Niet-media- en signaalbeveiligingsfuncties maken deel uit van de standaardinstallatie en vereisen geen tussenkomst van de gebruiker.

ITL en CTL

- ITL bevat de certificaatrol voor Call Manager TFTP, alle TVS-certificaten in het cluster en de functie Certificaatautoriteit Proxy (CAPF) wanneer uitgevoerd.
- CTL bevat vermeldingen voor System Administrator Security Token (SAST), Cisco CallManager en Cisco TFTP-services die op dezelfde server worden uitgevoerd, CAPF, TFTP-server(s) en Adaptive Security Applicatie (ASA) firewall. TVS wordt niet vermeld in CTL.

Certificaatregeneratieproces

> **Opmerking:** Alle endpoints moeten worden ingeschakeld en geregistreerd voordat de certificaten worden vernieuwd. Anders, vereisen de niet aangesloten telefoons de verwijdering van ITL.

Tomcat Certificate

Vermeld of certificaten van derden in gebruik zijn:

1. Navigeer naar elke server in uw cluster (in afzonderlijke tabbladen van uw webbrowser) begin met de uitgever, gevolgd door elke abonnee. Navigeer naar **Cisco Unified OS-beheer > Beveiliging > certificaatbeheer > Zoeken**.
   Waarschuwen uit de kolom Beschrijving als Tomcat zelfondertekend certificaat dat door systeem gegenereerd is. Als Tomcat door een derde partij is ondertekend, volg dan de link en voer deze stappen uit na de Tomcat-regeneratie.Door derden ondertekende certificaten, raadpleeg CUCM Upload CCMAdmin Web GUI Certificates.
2. Selecteer **Zoeken** om alle certificaten weer te geven: Selecteer het **Tomcat-**pem certificaat.Selecteer na het openen **Regenerate** en wacht tot u het pop-upvenster Success ziet, sluit vervolgens de pop-up of ga terug en selecteer **Zoeken/Lijst**.
3. Ga verder met elke volgende Subscriber, volg dezelfde procedure in stap 2 en vul alle Subscribers in uw cluster in.
4. Nadat alle knooppunten het Tomcat-certificaat opnieuw hebben gegenereerd, start u de Tomcat-service opnieuw op op alle knooppunten. Begin met de uitgever, gevolgd door de abonnees. Om Tomcat opnieuw te starten, moet u voor elke knooppunt een CLI-sessie openen en de **Opstart** van de **Opdrachtprogramma-service van Cisco Tomcat** uitvoeren.

```
admin:
admin:utils service restart Cisco Tomcat
 Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

5. Indien van toepassing zijn deze stappen vanuit de CCX-omgeving nodig:

- Als zelfondertekend certificaat wordt gebruikt, uploadt u de Tomcat-certificaten van alle knooppunten van het CUCM-cluster naar Unified CCX Tomcat-vertrouwenswinkel.
- Als CA ondertekend of privé CA ondertekend certificaat wordt gebruikt, upload wortel CA certificaat van CUCM naar Unified CCX Tomcat trust store.
- Start de servers opnieuw op zoals aangegeven in het certificaat en het regeneratiedocument voor CCX.

Aanvullende referenties:

- UCS Solution-certificaatbeheergids
- Unified CX Health Check Utility

IPSEC-certificaat

Opmerking: CUCM/Instant Messaging and Presence (IM&P) voor versie 10.X van de DRF Master Agent werkt op zowel CUCM Publisher als IM&P Publisher. DRF Lokale service wordt op de abonnees uitgevoerd. Versies 10.X en hoger, DRF Master Agent werkt alleen op de CUCM Publisher en op de lokale DRF-service op CUCM-abonnees en op IM&P Publisher en abonnees.

Opmerking: Het Disaster Recovery System maakt gebruik van een Secure Socket Layer (SSL)-gebaseerde communicatie tussen de Master Agent en Local Agent voor verificatie en codering van gegevens tussen de CUCM-clusterknooppunten. DRS maakt gebruik van de IPSec-certificaten voor de Public/Private Key-codering. Houd er rekening mee dat als u het bestand IPSEC truststore (hostname.pem) verwijdert van de pagina Certificaatbeheer, DRS niet werkt zoals verwacht. Als u het IPSEC-trust bestand handmatig verwijdert, moet u ervoor zorgen dat u het IPSEC-certificaat uploadt naar de IPSEC-vertrouwensopslag. Raadpleeg de Help-pagina voor certificaatbeheer in de Cisco Unified Communications Manager Security Guides voor meer informatie.

1. Navigeer naar elke server in uw cluster (in afzonderlijke tabbladen van uw webbrowser) begin met de uitgever, gevolgd door elke abonnee. Navigeren naar **Cisco Unified OS-beheer > Beveiliging > Certificaatbeheer > Zoeken**:
   Selecteer het **IPSEC-**pem certificaat.Selecteer na het openen **Regenerate** en wacht tot u het pop-upvenster Success ziet, sluit vervolgens de pop-up of ga terug en selecteer **Zoeken/Lijst**.
2. Doorgaan met volgende abonnees; volg dezelfde procedure in stap 1 en vul alle abonnees in uw cluster in.
3. Nadat alle knooppunten het IPSEC-certificaat opnieuw hebben gegenereerd, start u de services opnieuw op.
   Navigeer naar de Publisher **en Cisco Unified Service**. **Cisco Unified Service > Tools > Control Center - netwerkservices**.Selecteer **Opnieuw beginnen** op **Cisco DRF Master**dienst.Nadat het opnieuw opstarten van de service is voltooid, selecteert u **Herstart** op de **lokale service** van **Cisco DRF** op de uitgever, gaat u verder met de abonnees en selecteert u **Herstart** op de **lokale service van Cisco DRF**.

Het IPSEC.pem certificaat in de uitgever moet geldig zijn en moet aanwezig zijn in alle abonnees als IPSEC truststores. Het IPSEC.pem-certificaat van abonnees is niet aanwezig in de uitgever als IPSEC truststore in een standaardimplementatie. Om de geldigheid te verifiëren vergelijk de serienummers in het IPSEC.pem certificaat van de PUB met de IPSEC-trust in de SUBs. Ze moeten overeenkomen.

CAPF-certificaat

> **Waarschuwing**: Zorg ervoor dat u hebt geïdentificeerd als uw Cluster in Mixed-Mode is voordat u verdergaat. Verwijs naar sectie **Identificeer als uw cluster in Mix-Mode of Niet-beveiligde Mode is**.

1. Navigeer naar het **Cisco Unified CM-beheer > Systeem > Enterprise-parameters**. Controleer de sectie Security Parameters en controleer of de Cluster Security Mode is ingesteld op 0 of 1. Als de waarde 0 dan de cluster in de niet-beveiligde modus staat. Als het 1 is dan is het cluster in gemengde modus en moet u het CTL bestand bijwerken voorafgaand aan de herstart van de services. Zie Token- en Tokenless-koppelingen.
2. Navigeer naar elke server in uw cluster (in afzonderlijke tabbladen van uw webbrowser) begin met de uitgever, dan elke abonnee. Navigeer naar **Cisco Unified OS-beheer > Beveiliging > certificaatbeheer > Zoeken**.
   Selecteer het **CAPF pem** Certificate.Selecteer na het openen **Regenerate** en wacht tot u het pop-upvenster Success ziet, sluit vervolgens de pop-up of ga terug en selecteer **Zoeken/lijst**
3. Doorgaan met volgende abonnees; volg dezelfde procedure in stap 2 en vul alle abonnees in uw cluster in. Als het cluster alleen in de gemengde modus staat en de CAPF is geregenereerd - update de CTL voordat u verder gaat met Token - Tokenless.Als het cluster in de gemengde modus staat, moet de Call Manager-service ook opnieuw worden gestart voordat andere services opnieuw worden opgestart.
4. Nadat alle knooppunten het CAPF-certificaat hebben geregenereerd, start u de services opnieuw op.
   Navigeer naar de uitgever **Cisco Unified Service**. **Cisco Unified Service > Tools > Control Center - functieservices**.Begin met de uitgever en selecteer **Opnieuw beginnen** op de **Cisco Certificate Authority Proxy Functie Service** alleen waar actief.
5. Navigeer naar **Cisco Unified Service > Tools > Control Center - Network Services**. Begin met de uitgever en ga vervolgens door met de abonnees. Selecteer **Herstart** op **Cisco Trust Verification Service**. Navigeer naar **Cisco Unified Servicability > Tools > Control Center - Functieservices**.Begin met de uitgever en ga vervolgens door met de abonnees. Start **Cisco TFTP-service** alleen opnieuw waar actief.
6. Start alle telefoons opnieuw op: **Cisco Unified CM Management > Systeem > Enterprise-parameters**Selecteer **Reset** en vervolgens ziet u een pop-up met de verklaring **U staat op het punt alle apparaten in het systeem te resetten. Deze actie kan niet ongedaan worden gemaakt. Doorgaan?,** selecteer **OK** en selecteer vervolgens **Beginwaarden**.

De telefoons worden nu opnieuw ingesteld. Controleer hun acties via RTMT tool om te verzekeren dat de reset succesvol was en dat apparaten zich opnieuw registreren op CUCM. Wacht tot de telefoonregistratie is voltooid voordat u naar het volgende certificaat gaat. Dit proces van de registratie van telefoons kan wat tijd vergen. Let op: apparaten die slechte ITL's hadden voorafgaand aan het regeneratieproces, registreren niet terug naar het cluster totdat het wordt verwijderd.

CallManager-certificaat

> **Waarschuwing**: Zorg ervoor dat u hebt geïdentificeerd als uw Cluster in Mixed-Mode is voordat u verdergaat. Verwijs naar sectie **Identificeer als uw cluster in Mix-Mode of Niet-beveiligde Mode is**.

Waarschuwing: Regenereer CallManager.PEM- en TVS.PEM-certificaten niet tegelijkertijd. Dit veroorzaakt een onherstelbare mismatch met de geïnstalleerde ITL op endpoints die de verwijdering van ITL van ALLE endpoints in het cluster vereisen. Voltooi het gehele proces voor CallManager.PEM en zodra de telefoons terug zijn geregistreerd, start het proces voor de TVS.PEM.

1. Navigeer naar de **Cisco Unified CM Management > System > Enterprise Parameters**: Controleer de sectie Security Parameters en controleer of de Cluster Security Mode is ingesteld op 0 of 1. Als de waarde 0 dan de cluster in de niet-beveiligde modus staat. Als het 1 is dan is het cluster in gemengde modus en moet u het CTL bestand bijwerken voorafgaand aan de herstart van de services. Zie Token- en Tokenless-koppelingen.
2. Navigeer naar elke server in uw cluster (in afzonderlijke tabbladen van uw webbrowser) begin met de uitgever, dan elke abonnee. Navigeer naar **Cisco Unified OS-beheer > Beveiliging > certificaatbeheer > Zoeken**.
   Selecteer het CallManager-pem-certificaat.Selecteer na het openen **Regenerate** en wacht tot u het pop-upvenster Success ziet, sluit vervolgens de pop-up of ga terug en selecteer **Zoeken/Lijst**.
3. Doorgaan met volgende abonnees; volg dezelfde procedure in stap 2 en vul alle abonnees in uw cluster in. Als het cluster alleen in de gemengde modus staat en het CallManager-certificaat is hersteld - update de CTL voordat u verder gaat met Token - Tokenless
4. Meld u aan bij Publisher Cisco Unified Service: Navigeer naar **Cisco Unified Servicability > Tools > Control Center - Functieservices**.Begin met de uitgever en ga vervolgens door met de abonnees. Start **Cisco CallManager Service** opnieuw waar actief.
5. Navigeer naar **Cisco Unified Service > Tools > Control Center - functieservices**
   Begin met de uitgever en ga vervolgens met de abonnees verder. Start **Cisco CTIM Manager Service** alleen opnieuw waar actief.
6. Navigeer naar **Cisco Unified Service > Tools > Control Center - Network Services**.
   Begin met de uitgever en ga vervolgens door met de abonnees. Start **Cisco Trust Verification Service** opnieuw.
7. Navigeer naar **Cisco Unified Servicability > Tools > Control Center - Functieservices**.
   Begin met de uitgever en ga vervolgens door met de abonnees. Start **Cisco TFTP-service** alleen opnieuw waar actief.
8. Start alle telefoons opnieuw op: **Cisco Unified CM Management > Systeem > Enterprise-parameters**Selecteer **Reset** en vervolgens ziet u een pop-up met de verklaring **U staat op het punt alle apparaten in het systeem te resetten. Deze actie kan niet ongedaan worden gemaakt. Doorgaan?,** selecteer **OK** en selecteer vervolgens **Beginwaarden**

De telefoons worden nu opnieuw ingesteld. Controleer hun acties via RTMT tool om te verzekeren dat de reset succesvol was en dat apparaten zich opnieuw registreren op CUCM. Wacht tot de telefoonregistratie is voltooid voordat u naar het volgende certificaat gaat. Dit proces van de registratie van telefoons kan wat tijd vergen. Let op: apparaten die slechte ITL's hadden voorafgaand aan het regeneratieproces, registreren niet terug naar het cluster totdat ITL is verwijderd.

TV-certificaat

Waarschuwing: Regenereer CallManager.PEM- en TVS.PEM-certificaten niet tegelijkertijd. Dit veroorzaakt een onherstelbare mismatch met de geïnstalleerde ITL op endpoints die de verwijdering van ITL van ALLE endpoints in het cluster vereisen.

Opmerking: TVS certificeert certificaten namens Call Manager. Herstel dit certificaat als laatste.

Navigeer naar elke server in uw cluster (in afzonderlijke tabbladen van uw webbrowser) begin met de uitgever, dan elke abonnee. Navigeren naar **Cisco Unified OS-beheer > Beveiliging > Certificaatbeheer > Zoeken**:

- Selecteer het **TVS pem** Certificate.
- Selecteer na het openen **Regenerate** en wacht tot u het pop-upvenster Success ziet, sluit vervolgens de pop-up of ga terug en selecteer **Zoeken/Lijst**.

1. Doorgaan met volgende abonnees; volg dezelfde procedure in stap 1 en vul alle abonnees in uw cluster in. Nadat alle knooppunten het TVS-certificaat opnieuw hebben gegenereerd, start u de services opnieuw: Meld u aan bij Publisher **en Cisco Unified Service**. Navigeer naar **Cisco Unified Service > Tools > Control Center - Network Services**.Selecteer in de uitgeverij **Herstart** op **Cisco Trust Verification Service**.Nadat de service is herstart, gaat u door met de abonnees en start u de **Cisco Trust Verification Service** opnieuw.
2. Begin met de uitgever en ga vervolgens door met de abonnees. Start alleen de **Cisco TFTP-service** opnieuw waar actief.
3. Start alle telefoons opnieuw op: **Cisco Unified CM Management > Systeem > Enterprise Parameters**.Selecteer **Reset** en vervolgens ziet u een pop-up met de verklaring **U staat op het punt alle apparaten in het systeem te resetten. Deze actie kan niet ongedaan worden gemaakt. Doorgaan?,** selecteer **OK** en selecteer vervolgens **Beginwaarden**.

De telefoons worden nu opnieuw ingesteld. Controleer hun acties via RTMT tool om te verzekeren dat de reset succesvol was en dat apparaten zich opnieuw registreren op CUCM. Wacht tot de telefoonregistratie is voltooid voordat u naar het volgende certificaat gaat. Dit proces van de registratie van telefoons kan wat tijd vergen. Let op: apparaten die slechte ITL's hadden voorafgaand aan het regeneratieproces, registreren niet terug naar het cluster totdat ITL is verwijderd.

ITLR-herstelcertificaat

Opmerking: Het ITLRecovery-certificaat wordt gebruikt wanneer apparaten hun vertrouwde status verliezen. Het certificaat verschijnt in zowel het ITL als de CTL (wanneer de CTL-provider actief is).
Als apparaten hun vertrouwensstatus verliezen, kunt u de opdracht **hulpprogramma's itl reset localkey** gebruiken voor niet-beveiligde clusters en de opdracht **hulpprogramma's ctl reset localkey** voor mix-mode clusters. Lees de beveiligingshandleiding voor uw Call Manager-versie om vertrouwd te raken met de manier waarop het ITLR-herstelcertificaat wordt gebruikt en het proces dat nodig is om de vertrouwde status te herstellen.
Als het cluster is opgewaardeerd naar een versie die een sleutellengte van 2048 ondersteunt en de clusterservercertificaten zijn terugveranderd in 2048 en de terugwinning van de ITLR niet is geregenereerd en momenteel een sleutellengte van 1024 heeft, is de opdracht voor herstel van het ITL mislukt en wordt de methode voor herstel van de ITLR niet gebruikt.

1. Navigeer naar elke server in uw cluster (in afzonderlijke tabbladen van uw webbrowser) begin met de uitgever, dan elke abonnee. Navigeren naar **Cisco Unified OS-beheer > Beveiliging > Certificaatbeheer > Zoeken**:
   Selecteer het **ITLR-pem** certificaat voor herstel.Selecteer na het openen **Regenerate** en

wacht tot u het pop-upvenster Success ziet, sluit vervolgens de pop-up of ga terug en selecteer **Zoeken/Lijst**.
2. Doorgaan met volgende abonnees; volg dezelfde procedure in stap 2 en vul alle abonnees in uw cluster in.
3. Nadat alle knooppunten het ITLR-herstelcertificaat opnieuw hebben gegenereerd, moeten de services als volgt worden herstart: Als u in Gemengde modus bent - update de CTL voordat u verdergaat met Token - Tokenless.Meld u aan bij Publisher **Cisco Unified Service**. Navigeer naar **Cisco Unified Service > Tools > Control Center - Network Services**.Selecteer in de uitgeverij **Herstart** op **Cisco Trust Verification Service**. Nadat de service is herstart, gaat u door met de abonnees en start u de **Cisco Trust Verification Service** opnieuw.
4. Begin met de uitgever en ga vervolgens door met de abonnees. Start alleen de **Cisco TFTP-service** opnieuw waar actief.
5. Start alle telefoons opnieuw op: **Cisco Unified CM Management > Systeem > Enterprise-parameters**Selecteer **Reset** en vervolgens ziet u een pop-up met de verklaring **U staat op het punt alle apparaten in het systeem te resetten. Deze actie kan niet ongedaan worden gemaakt. Doorgaan?,** selecteer **OK** en selecteer vervolgens **Beginwaarden**.
6. Telefoons uploaden nu de nieuwe ITL/CTL terwijl ze resetten.

Verlopen vertrouwenscertificaten verwijderen

Opmerking: Identificeer de vertrouwenscertificaten die moeten worden verwijderd, niet langer nodig zijn of verlopen zijn. Verwijder de vijf basiscertificaten die CallManager.pem, tomcat.pem, ipsec.pem, CAPF.pem en TVS.pem bevatten niet. Vertrouwenscertificaten kunnen indien nodig worden verwijderd. De volgende dienst die herstart is ontworpen om informatie over oude certificaten binnen die diensten te wissen.

1. Navigeer naar **Cisco Unified Service > Tools > Control Center - Network Services**. Selecteer in de vervolgkeuzelijst de CUCM Publisher.Selecteer **Kennisgeving stop-certificaatwijziging**.Herhaal dit voor elke Call Manager-knooppunt in uw cluster.Als u een IMP-server hebt: Selecteer in het uitrolmenu uw IMP-servers één voor één en selecteer **Stop Platform Management Web Services en Cisco Intercluster Sync Agent**.
2. Navigeer naar **Cisco Unified OS-beheer > Beveiliging > certificaatbeheer > Zoeken**. Vind de verlopen vertrouwenscertificaten. (Voor versies 10.X en hoger kunt u filteren op Vervaldatum. Voor versies lager dan 10.0 moet u de specifieke certificaten handmatig of via de RTMT-waarschuwingen indien ontvangen.)Hetzelfde vertrouwenscertificaat kan in meerdere knooppunten verschijnen. Het moet van elk knooppunt afzonderlijk worden verwijderd.Selecteer het certificaat dat moet worden verwijderd (afhankelijk van uw versie krijgt u een pop-up of u navigeerde naar het certificaat op dezelfde pagina) Selecteer **Verwijderen**. (U krijgt een pop-up die begint met "u staat op het punt dit certificaat permanent te verwijderen".*)*Selecteer **OK**.
3. Herhaal het proces voor elk vertrouwenscertificaat dat moet worden verwijderd.
4. Na voltooiing moeten de diensten die rechtstreeks verband houden met de verwijderde certificaten worden hervat. U hoeft de telefoons in deze sectie niet opnieuw op te starten. Call Manager en CAPF kunnen invloed hebben op endpoints. Tomcat-trust: start Tomcat Service opnieuw via opdrachtregel (zie Tomcat-sectie)CAPF-trust: Cisco Certificate Authority Proxy-functie opnieuw opstarten (zie CAPF-sectie). Start geen endpoints opnieuw op.CallManager-trust: CallManager Service/CTIM Manager (zie het gedeelte CallManager)

start de endpoints niet opnieuw op. Effecten op eindpunten en oorzaken opnieuw beginnen.IPSEC-trust: DRF Master/DRF lokaal (zie IPSEC-sectie).TVS (zelfondertekend) heeft geen vertrouwenscertificaten.

5. Eerder gestopt Start Services in Stap 1.

Verificatie

Voor deze configuratie is geen verificatieprocedure beschikbaar.

Problemen oplossen

Er zijn geen procedures voor probleemoplossing beschikbaar voor deze configuratie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.