

Hergebruik van multi-SAN Tomcat-certificaat voor CallManager implementeren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Tomcat-certificaat voor CallManager opnieuw gebruiken](#)

[Verifiëren](#)

Inleiding

Dit document beschrijft een stap-voor-stap proces voor het hergebruiken van het Multi-SAN Tomcat-certificaat voor CallManager op CUCM.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Communications Manager (CUCM)
- CUCM-certificaten
- Identity Trust List (ITL)

Gebruikte componenten

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

- CUCM release 15 SU1

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.

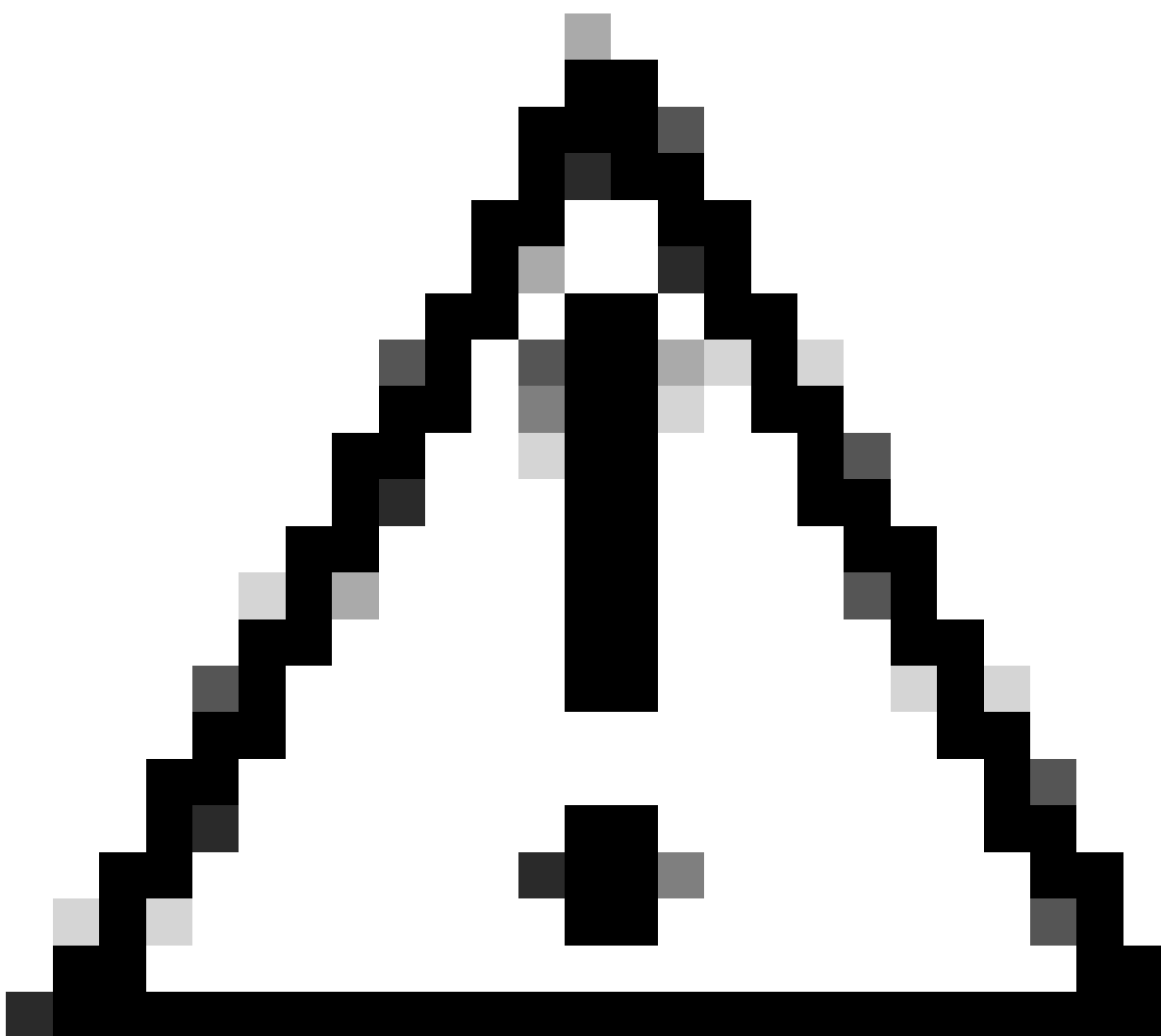
Achtergrondinformatie

Eerdere versies van CUCM gebruikten verschillende certificaten voor elke dienst voor de volledige

cluster, waardoor het aantal certificaten en de kosten toenamen. Dit omvat Cisco Tomcat en Cisco CallManager die kritieke services zijn die worden uitgevoerd op CUCM en die ook over respectieve identiteitscertificaten beschikken.

Beginnend met CUCM versie 14, werd een nieuwe eigenschap toegevoegd om het multi-SAN Tomcat-certificaat voor CallManager-service te hergebruiken.

Het voordeel van deze functie is dat u één certificaat van de CA kunt verkrijgen en het voor meerdere toepassingen kunt gebruiken. Dit garandeert kostenoptimalisatie en een reductie van het beheer en beperkt de omvang van het ITL-bestand, waardoor de overheadkosten worden beperkt.



Waarschuwing: voordat u verder gaat met de configuratie van het hergebruik, moet u ervoor zorgen dat Tomcat-certificaat een SAN-certificaat voor meerdere servers is. Tomcat Multi-SAN-certificaat kan zelfondertekend of CA-ondertekend zijn.

Configureren

Tomcat-certificaat voor CallManager opnieuw gebruiken



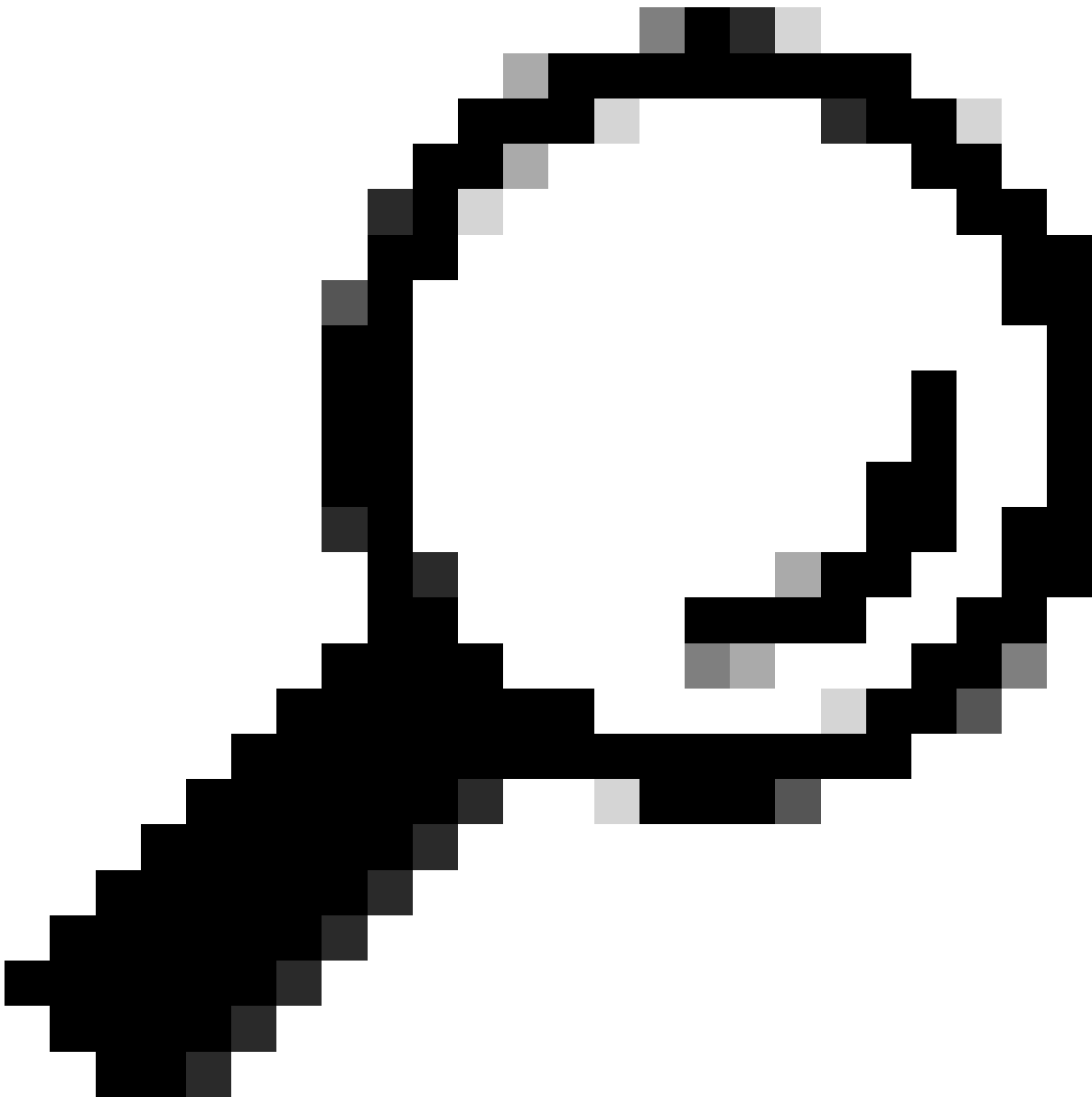
Waarschuwing: Zorg ervoor dat u hebt geïdentificeerd of uw cluster in de gemengde of niet-beveiligde modus staat voordat u verdergaat.

Stap 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 is, is het cluster in de niet-beveiligde modus. Als het 1 is, dan is het cluster in gemengde modus en u moet het CTL bestand bijwerken voorafgaand aan de herstart van de services.

Stap 2. Navigeer naar uw CUCM-uitgever en vervolgens naar Cisco Unified OS-beheer > Beveiliging > certificaatbeheer.

Stap 3. Upload Multi-SAN Tomcat CA Certificaatketen naar CallManager Trust Store.



Tip: als u een zelfondertekend multi-server SAN-certificaat voor Tomcat gebruikt, kunt u deze stap overslaan.

Alvorens de certificaten te hergebruiken, zorg ervoor dat u handmatig de CA-certificaatketen (die het tomcat-identiteitscertificaat ondertekende) uploadt naar de CallManager-vertrouwenwinkel.

Start deze services opnieuw wanneer u de tomcat-certificaatketen uploadt naar het CallManager-vertrouwen.

- CallManager: Cisco HAProxy-service
- CallManager-ECDSA: Cisco CallManager-service en Cisco HAProxy-service

Stap 4. Klik op Certificaat van hergebruik. De pagina Tomcat-certificaten voor andere services gebruiken wordt weergegeven.

Use Tomcat Certificate For Other Services



Finish



Close

Status



Tomcat-ECDSA Certificate is Not Multi-Server Certificate



Tomcat Certificate is Multi-Server Certificate

Source

Choose Tomcat Type*

tomcat



Replace Certificate for the following purpose



CallManager



CallManager-ECDSA

Finish

Close

Stap 5. Kies in de vervolgkeuzelijst Tomcat-type de optie Tomcat of de optie Tomcat-ECDSA.



Stap 6. Selecteer in het volgende deelvenster Certificaat vervangen het aanvinkvakje CallManager of CallManager-ECDSA op basis van het geselecteerde certificaat in een eerdere stap.






Opmerking: Als u Tomcat als certificaatype kiest, wordt CallManager ingeschakeld als vervanging. Als u tomcat-ECDSA als certificaatype kiest, wordt CallManager-ECDSA ingeschakeld als vervanging.

Stap 7. Klik op Voltooien om het CallManager-certificaat te vervangen door het nieuwe SAN-certificaat met meerdere servers.

Use Tomcat Certificate For Other Services

 Finish  Close

Status

-  Certificate Successful Provisioned for the nodes cucmpub15. , cucmsub15. .
-  Restart Cisco HAProxy Service for the generated certificates to become active.
-  If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.

Stap 8. Start de Cisco HAProxy-service op alle knooppunten van het cluster opnieuw door de utils-service uit te voeren en de Cisco HAProxy-opdracht via CLI opnieuw te starten.

```
admin:utils service restart Cisco HAProxy
Stopping Cisco HAProxy...

Cisco HAProxy [STOPPED] Service Activated
Starting Cisco HAProxy...
Cisco HAProxy [STARTED]
admin: █
```

Stap 9. Als het cluster in de gemengde modus staat, werkt u het CTL-bestand bij door commando-hulpprogramma's ctl update CTLF-bestand via CLI van CUCM Publisher uit te voeren en gaat u verder met het resetten van de telefoons om het nieuwe CTL-bestand te krijgen.

Verifiëren

Opmerking: het CallManager-certificaat wordt niet weergegeven op GUI wanneer u het certificaat opnieuw gebruikt.

U kunt de opdracht uitvoeren vanaf de CLI om te bevestigen dat CallManager het Tomcat-certificaat hergebruikt.

- cert list eigen tonen

```
admin:show cert list own
tomcat/tomcat.pem: Certificate Signed by AKASH-WINSERVLAB-CA
tomcat-ECDSA/tomcat-ECDSA.pem: Self-signed certificate generated by system
ipsec/ipsec.pem: Self-signed certificate generated by system
ITLRecovery/ITLRecovery.pem:
CallManager-ECDSA/CallManager-ECDSA.pem: Self-signed certificate generated by system
CallManager/CallManager.pem: Reusing tomcat certificate for CallManager
TVS/TVS.pem: Self-signed certificate generated by system
admin:█
```


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.