Tomcat Certificate Reuse configureren voor CallManager in CUCM 14

Inhoud

Inleiding

In dit document wordt beschreven hoe u het Multi-SAN Tomcat-certificaat voor CallManager opnieuw kunt gebruiken op een Cisco Unified Communications Manager (CUCM)-server.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CUCM-certificaten
- Real-time Monitoring Tool (RTMT)
- Identiteitsvertrouwenslijst (ITL)

Gebruikte componenten

De informatie in dit document is gebaseerd op CUCM 14.0.1.13900-155.

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

De twee belangrijkste diensten voor CUCM zijn Tomcat en CallManager. In de eerdere versies waren voor elke service verschillende certificaten vereist voor het volledige cluster. In CUCM-versie 14 is een nieuwe functie toegevoegd om ook het Multi-SAN Tomcat-certificaat voor CallManager-service te hergebruiken. De voordelen van het gebruik van deze functie zijn:

- Verlaagt de kosten van het verkrijgen van twee certificaten ondertekend door een Public Certificate Authority (CA) voor één cluster van CA-ondertekende certificaten.
- Deze functie verkleint de grootte van het ITL-bestand, waardoor de overhead wordt verminderd.

Low Impact Medium Impact. High Impact.

Type	Risk	Trust List	Impact	Phone Restart	Service Restart
Tomcat		-	Web services, SSO, EM/EMCC Login	None	Tomcat
IPSec		-	DRS, Ipsec Tunnels	None	DRF Master/Local
CAPF		CTL + ITL	LSC must be updated, secure features	All	CAPF
Callmanager		CTL + ITL	Registration, TL issues, Trunks, CTI	All	CM,CTI,TFTP
TVS		ITL	Verification of TLs, CFG files, https connection	Some	TVS
ITLRecovery		CTL + ITL	Signer or SAST backup for ITL/CTL	All	

Configureren

Let op: Controleer of Single Sign-on (SSO) is uitgeschakeld voordat u een Tomcat-certificaat uploadt. Als deze optie is ingeschakeld, moet SSO worden uitgeschakeld en opnieuw worden ingeschakeld zodra het regeneratieproces van het Tomcat-certificaat is voltooid.

1. Tomcat-certificaat instellen als Multi-SAN Low Impact

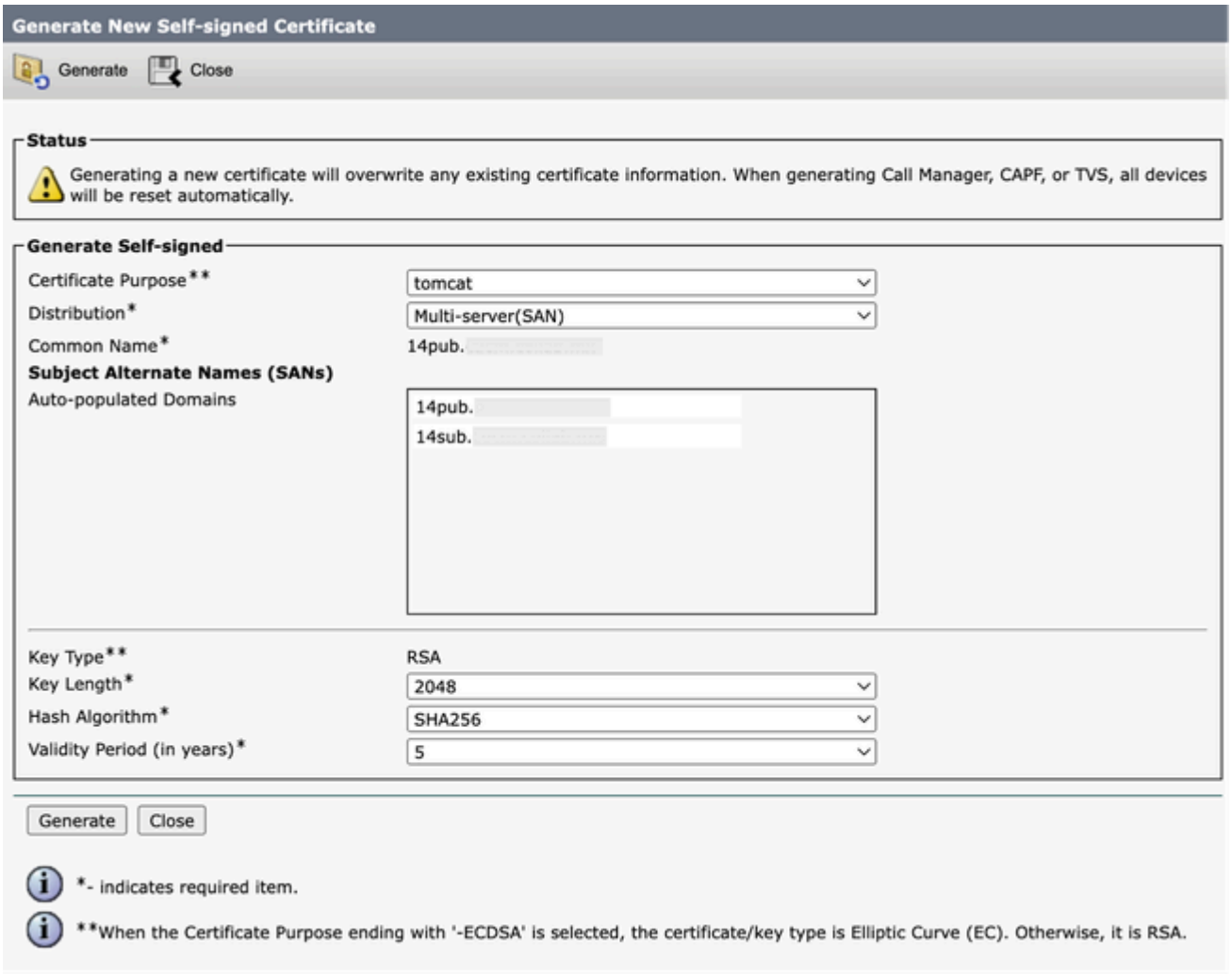
In CUCM 14 kan het Tomcat Multi-SAN-certificaat zelfondertekend of CA-ondertekend zijn. Als uw Tomcat-certificaat al Multi-SAN is, slaat u deze sectie over.

zelfondertekend

Stap 1. Log in bij Publisher > Operating System (OS) Administration en navigeer naar Security > Certificate Management >

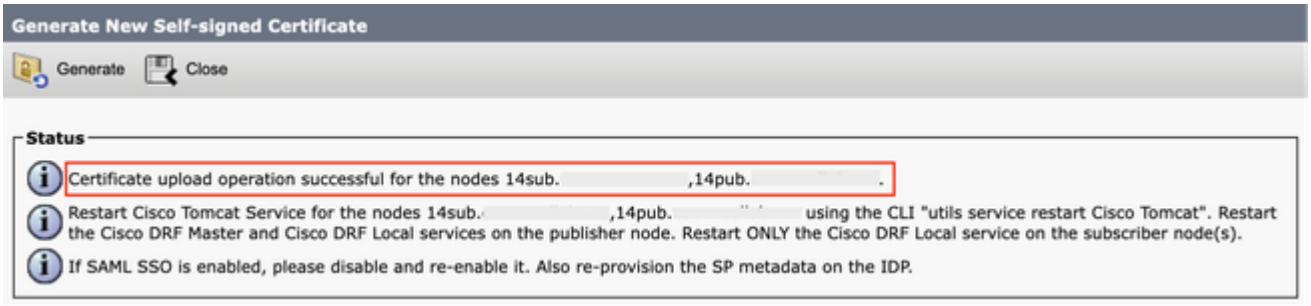
Generate Self-Signed.

Stap 2. Kies Certificate Purpose: tomcat > Distribution: Multi-Server SANuit. De SAN-domeinen en het bovenliggende domein worden automatisch gevuld.



Scherm met zelfondertekend Multi-SAN Tomcat-certificaat genereren

Stap 3. Klik op Generateen bevestig dat al uw knooppunten onder het Certificate upload operation successful bericht worden vermeld. Klik op de knop .Close



Succesvol bericht voor zelfondertekende Multi-SAN Tomcat genereren

Stap 4. Start de Tomcat-service opnieuw op, open een CLI-sessie voor alle nodes van het cluster en voer deutils service restart Cisco Tomcatopdracht uit.

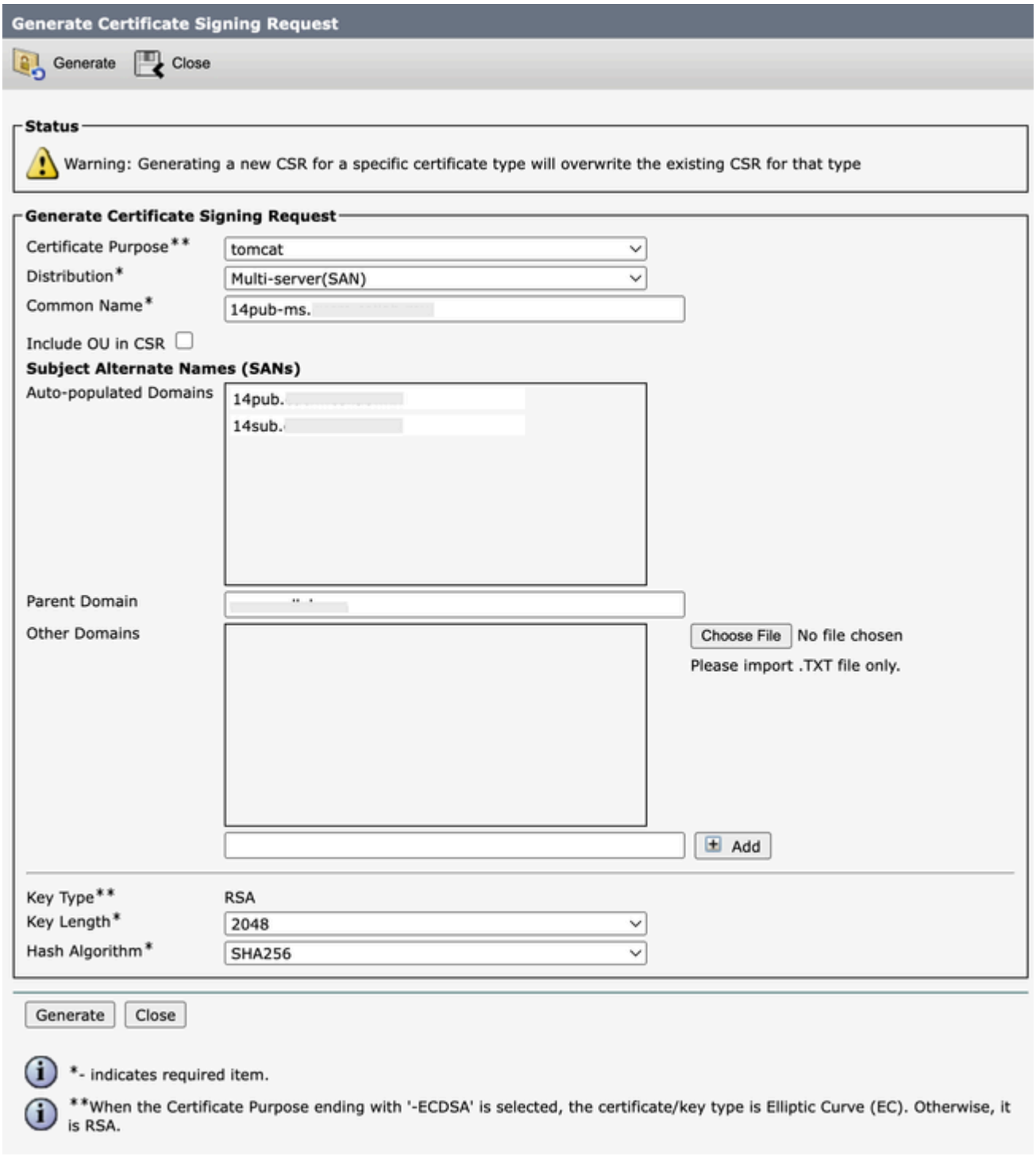
Stap 5. Navigeer naar het Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services scherm en start de Cisco DRF Master Service en Cisco DRF Local Service.

Stap 6. Navigeer naar elk Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services en start opnieuw Cisco DRF Local Service.

CA-ondertekend

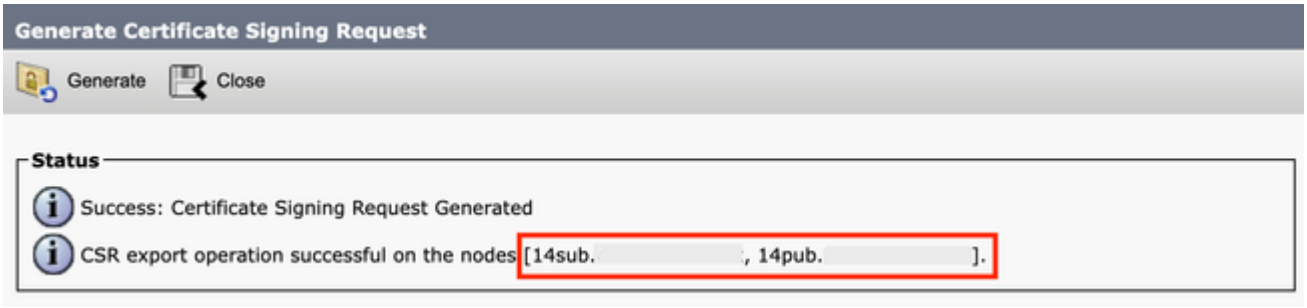
Stap 1. Log in bij Publisher > Operating System (OS) Administration en navigeer naar Security > Certificate Management > Generate CSR.

Stap 2. Kies Certificate Purpose: tomcat > Distribution: Multi-Server SANuit. De SAN-domeinen en het bovenliggende domein worden automatisch gevuld.



Multi-SAN CSR genereren voor Tomcat-certificaatscherm

Stap 3. Klik op Generateen valideer dat al uw knooppunten onder het bericht worden CSR export operation successful vermeld. Klik op de knop . Close



Succesvol bericht over Multi-SAN CSR Tomcat genereren

Stap 4. Klik op de knop . Download CSR > Certificate Purpose: tomcat > Download

Scherm MVO van Tomcat downloaden

Stap 5. Stuur de CSR naar uw CA voor ondertekening.

Stap 6. Om de CA-vertrouwensketen te uploaden, navigeert u Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust. Stel de beschrijving van het certificaat in en blader door de bestanden van de vertrouwensketen.

Stap 7. Upload het certificaat met CA-handtekening en navigeer naar Certificate Management > Upload certificate > Certificate Purpose: tomcat. Stel de beschrijving van het certificaat in en blader door het CA-ondertekende certificaatbestand.

Stap 8. Start de Tomcat-service opnieuw op, open een CLI-sessie voor alle nodes van het cluster en voer de opdracht utils service restart Cisco Tomcat uit.

Stap 9. Navigeer naar het Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services scherm en start de Cisco DRF Master Service en Cisco DRF Local Service.

Stap 10. Navigeer naar elk Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services en start opnieuw Cisco DRF Local Service.

2. Tomcat-certificaat opnieuw gebruiken voor CallManager

Medium Impact.

⚠

Let op: voor CUCM 14 wordt een nieuwe bedrijfsparameter Phone Interaction on Certificate Update ingevoerd. Gebruik dit veld om telefoons handmatig of automatisch opnieuw in te stellen wanneer een van de TVS-, CAPF- of TFTP-certificaten (CallManager/ITLRrecovery) wordt bijgewerkt. Deze parameter is standaard ingesteld op reset the phones automaticallyInstellingen. Na regeneratie, verwijdering en update van certificaten moet u ervoor zorgen dat de juiste services opnieuw worden gestart.

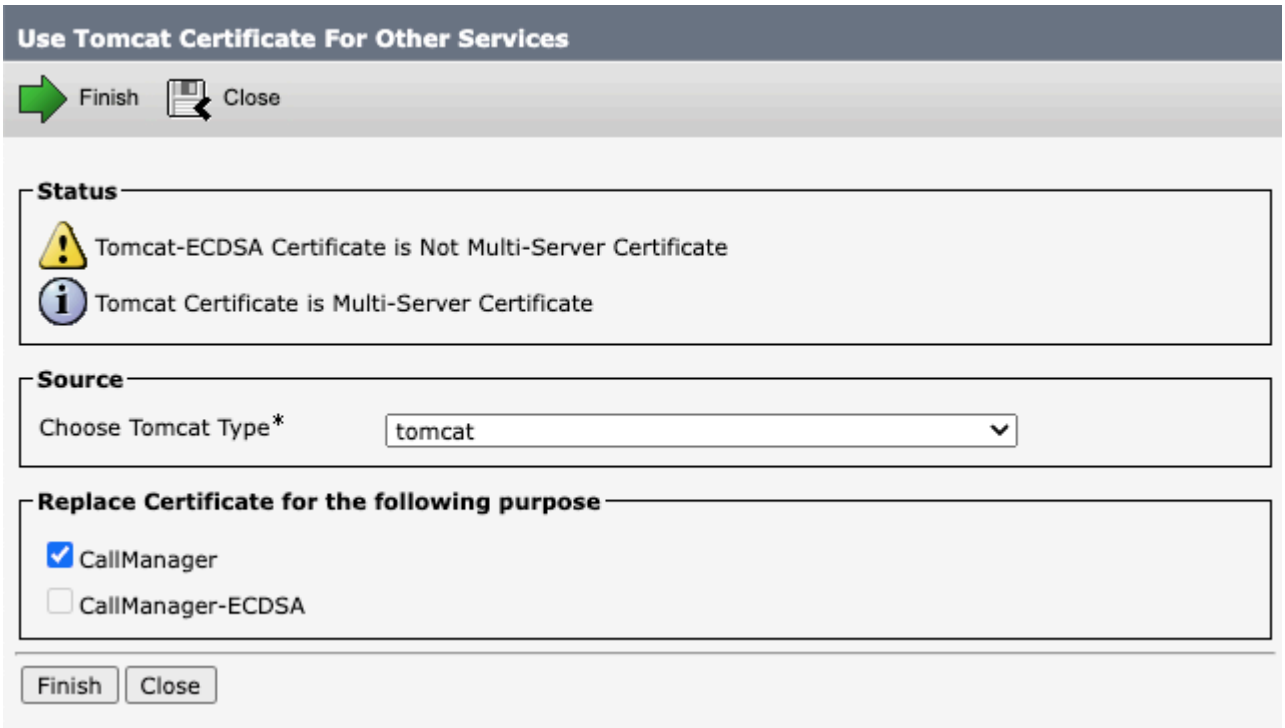
Herstart van de services voor een normale CallManager-certificaatregeneratie is vereist. Controleer Certificaten opnieuw genereren in Unified Communications Manager.

Stap 1. Navigeer naar uw CUCM-uitgever en vervolgens naar Cisco Unified OS Administration > Security > Certificate Management.

Stap 2. Klik op de knop . Reuse Certificate

Stap 3. Kies in de choose **Tomcat type** vervolgkeuzelijst tomcat.

Stap 4. Vink het selectievakje aan in het Replace Certificate for the following purpose deelvenster CallManager.

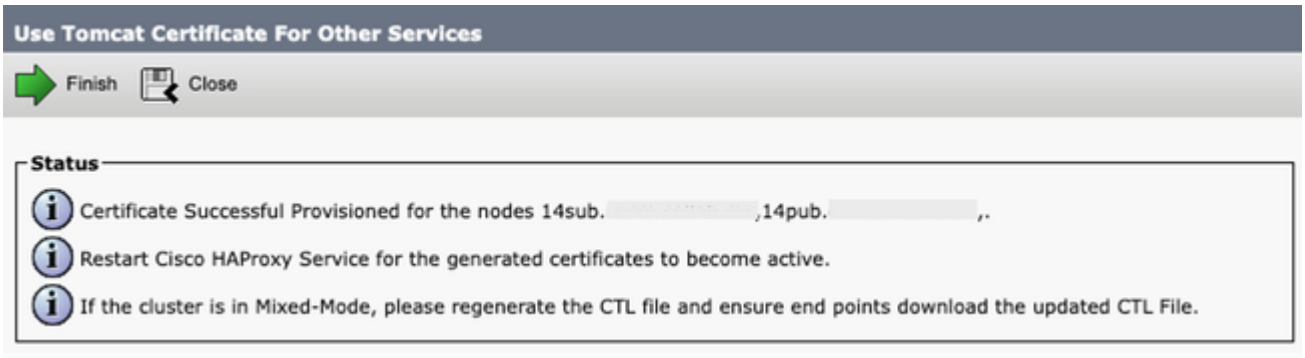


Scherm Tomcat-certificaat voor andere services hergebruiken

Opmerking: Als u Tomcat kiest als certificaattype, is CallManager ingeschakeld als vervanging. Als u tomcat-ECDSA als certificaattype kiest, is CallManager-ECDSA ingeschakeld als vervanging.

Stap 5. Klik op Finish om het CallManager-certificaat te vervangen door het Tomcat Multi-SAN-

certificaat.



Bericht over geslaagd Tomcat-certificaat opnieuw gebruiken

Stap 6. Start de Cisco HAProxy-service opnieuw op, open een CLI-sessie naar alle nodes van het cluster en voer de opdracht utils service restart Cisco HAProxy uit.

Opmerking: om te bepalen of het cluster zich in de gemengde modus bevindt, gaat u naar Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == niet-beveiligd; 1 == gemengde modus).

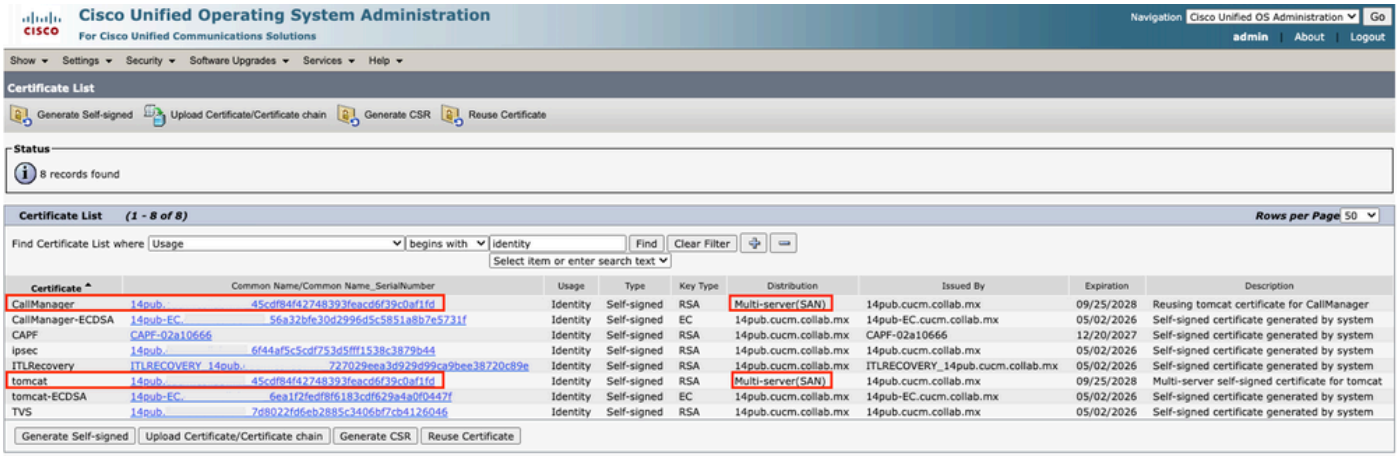
Stap 7. Als uw cluster zich in de gemengde modus bevindt, opent u een CLI-sessie naar de Publisher-node en voert u de opdracht uit en stelt u alle telefoons van het cluster opnieuw in zodat de CTL-bestandsupdates **utils ctl update CTLFile** van kracht worden.

Verifiëren

Stap 1. Navigeer naar uw CUCM-uitgever en vervolgens naar Cisco Unified OS Administration > Security > Certificate Management.

Stap 2. Filter op Find Certificate List where: Usage > begins with: identity en klik op Find.

Stap 3. CallManager- en Tomcat-certificaten moeten eindigen met dezelfde Common Name_Serial Number waarde.



Opmerking: vanaf SU4 wordt het Call Manager-certificaat niet weergegeven op de GUI, terwijl beide certificaten zichtbaar zijn in SU2 en SU3.

Gerelateerde informatie

- Beveiligingsgids voor Cisco Unified Communications Manager 14
- Cisco Technical Support en downloads

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.