Een door CA ondertekende alternatieve naam voor meerdere servers in CVOS-systemen configureren

Inhoud

Inleiding

In dit document wordt beschreven hoe u een Cisco Voice Operating System (CVOS)-systeemcluster kunt configureren met behulp van een door Certificaatinstantie (CA) ondertekende multi-server subject Alternate Name (SAN) met uitgever - Subscriber Architecture model. Het CVOS-systeem omvat CUIC, Finesse, Livedata, IDs-systemen in UCCE-omgeving.

Bijgedragen door Venu Gopal Sane, Ritesh Desai Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Contact Center Enterprise (UCS) release v12.5
- Cisco Packet Contact Center Enterprise (PCE) release v12.5
- Cisco Finesse v12.5
- Cisco Unified Intelligence Center v12.5

Gebruikte componenten

De informatie in dit document is gebaseerd op CVOS Operating System Administration - Certificate Management.

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 de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Met multi-server SAN-certificaten hoeft slechts één CSR te worden ondertekend door CA voor één cluster van knooppunten, in plaats van de vereiste om een CSR te verkrijgen van elke serverknooppunt van de

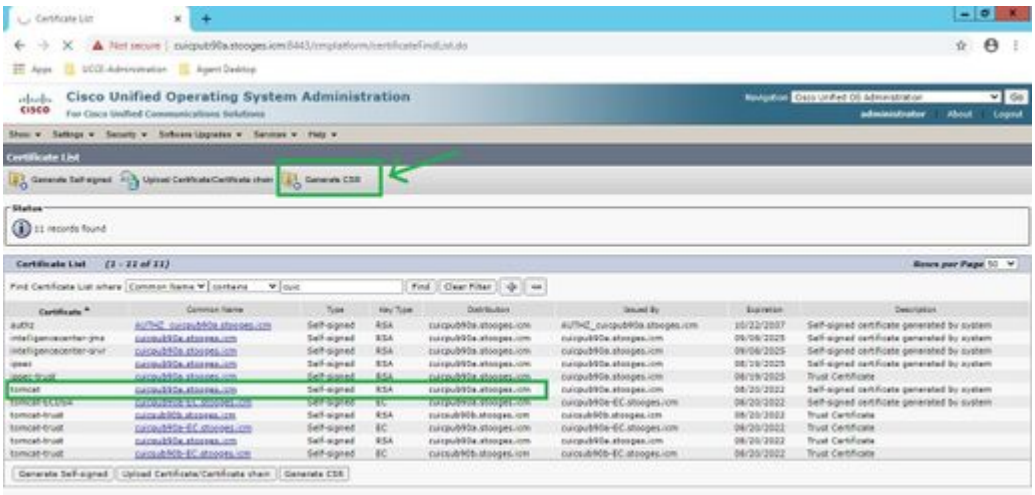
cluster en vervolgens een CA-ondertekend certificaat te verkrijgen voor elke CSR en deze individueel te beheren.

Zorg er voordat u deze configuratie probeert voor dat deze services zijn ingesteld en functioneel zijn:

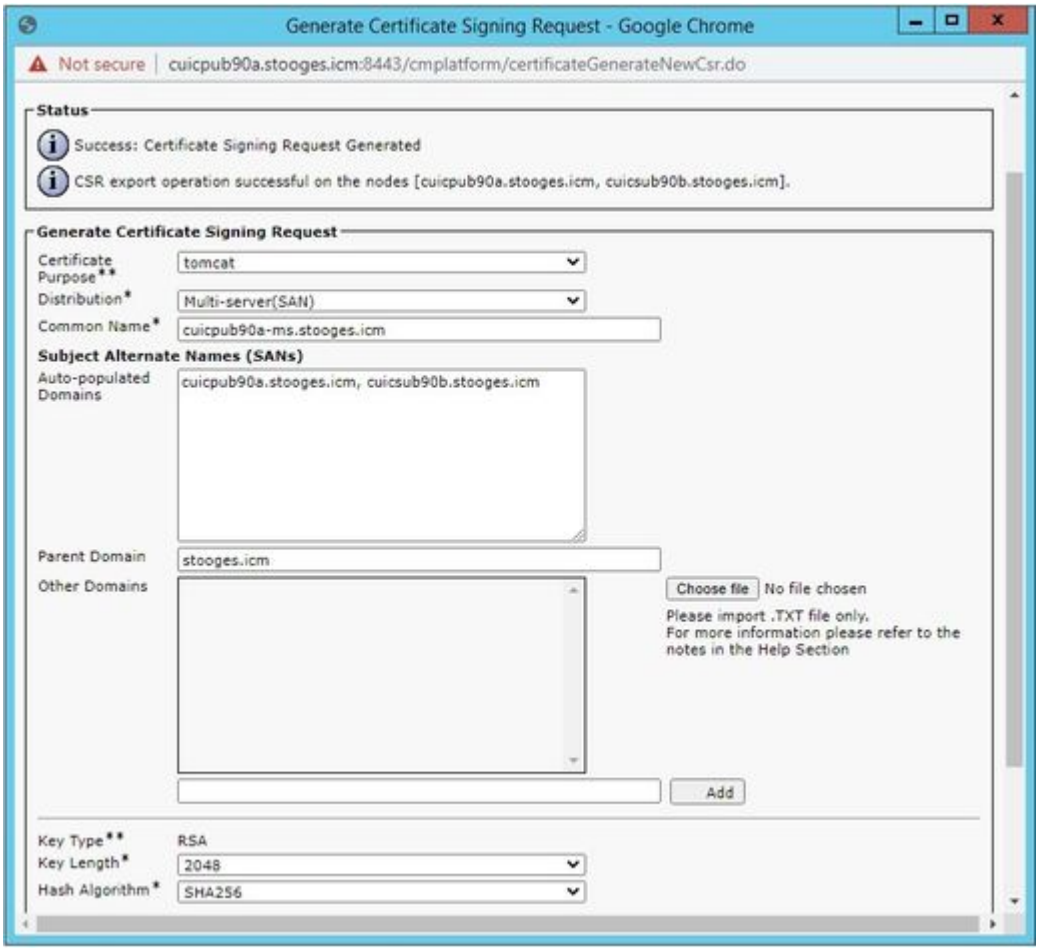
- Cisco Tomcat-service
- Kennisgeving van Cisco-certificaatwijziging
- Cisco-monitor voor certificaatverloop

Configureren

Stap 1. Log in Besturingssysteem (OS) administratie en navigeer naar **Beveiliging > Certificaatbeheer > Generate CSR** zoals getoond in het afbeelding.

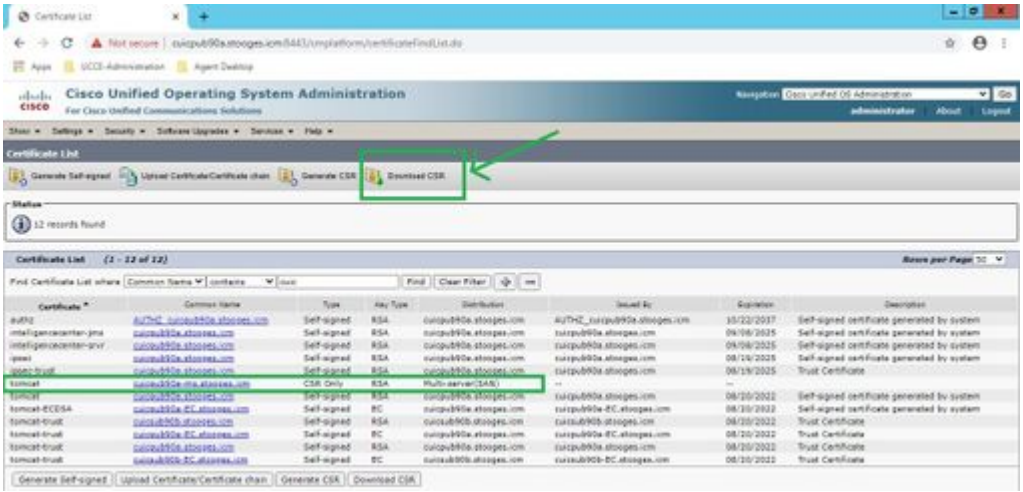


Stap 2. Selecteer een **SAN met meerdere servers** in distributie. De SAN-domeinen en het parent-domein worden automatisch ingevuld.

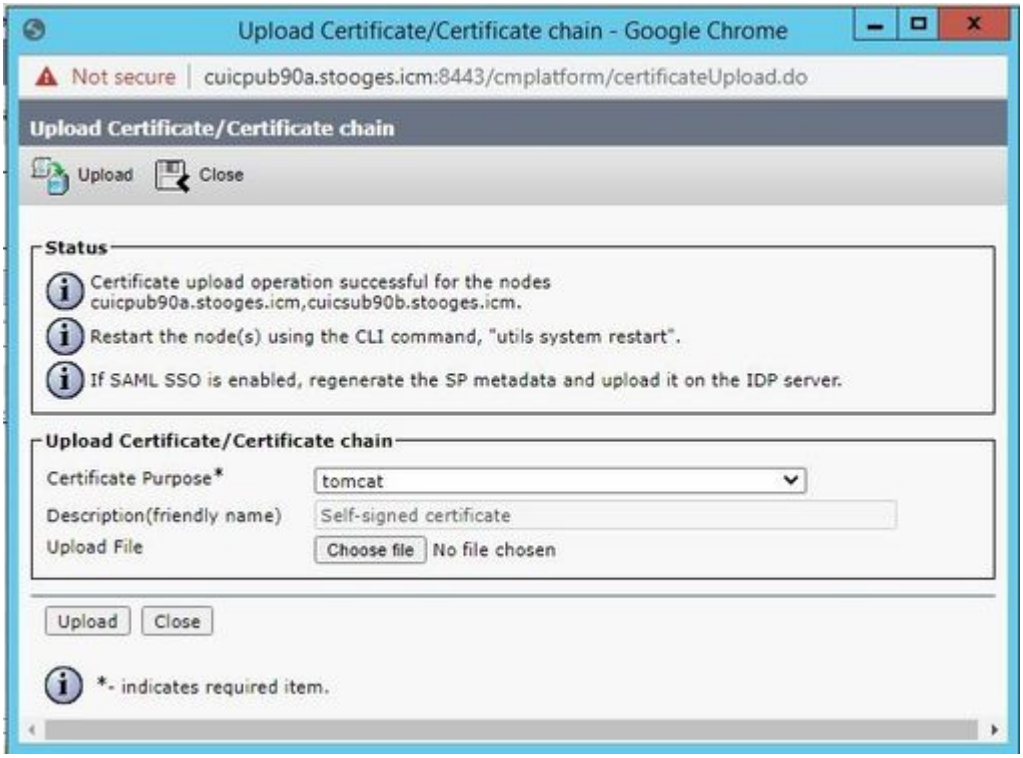


Stap 3. Een succesvolle generatie van MVO laat deze boodschap zien:

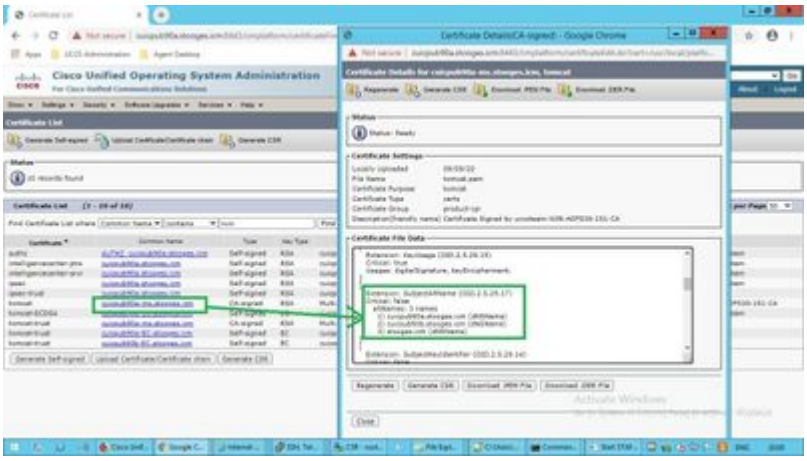
Stap 4. Na een succesvolle generatie van MVO, kan gegenereerde MVO hier worden gezien, die kan worden gedownload naar CA voor ondertekening.



Stap 5. Upload het CA-ondertekende certificaat als type naar de Publisher-knooppunt van het cluster op de pagina voor certificaatbeheer en volg de instructies die worden weergegeven na een succesvolle uploadprocedure.



Stap 6. Nadat het bestand is geüpload, controleert u de certificaatlijst met het nieuwe CA-ondertekende certificaat als type multi-SAN.



Klik op het nieuwe multi-SAN-certificaat, controleer of OnderwerpAltNames Domeinnaam en FQDNâ€™s van alle clusterknooppunten toont.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Meld u aan bij **platform** page van Subscriber-knooppunten en controleer of hetzelfde multi-SAN-certificaat is ingevuld met het gebruik van http://<any-node-fqdn>:8443/platform.

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Verzamel deze logboeken voor certificaatbeheer van CLI-toegang en open de case met Cisco TAC: **file get activelog platform/log/cert***

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.