CSR genereren en certificaten op CMS toepassen

Inhoud

Inleiding

Dit document beschrijft hoe u een verzoek voor certificaatondertekening (CSR) kunt genereren en ondertekende certificaten kunt uploaden naar Cisco Meeting Server (CMS).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van CMS Server

Gebruikte componenten

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

- Putty of soortgelijke software
- CMS 2.9 of 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.

Genereer de CSR

Er zijn twee manieren waarop u CSR kunt genereren, één daarvan is om de CSR direct op de CMS server te genereren via Command Line Interface (CLI) met admin toegang, de andere is om het te doen met externe 3rd party Certificate Authority (CA) zoals Open SSL.

In beide gevallen moet MVO met de juiste syntaxis worden gegenereerd om MCS-diensten goed te laten werken.

Stap 1. Syntaxisstructuur.

```
pki csr <key/cert basename> <CN:value> [OU:<value>] [O:<value>] [ST:<-value>] [C:<value>] [subjectAltNam
```

- <key/cert basename> is een string die de nieuwe key en CSR naam identificeert. Het kan alfanumerieke, koppelteken of onderstreepteken tekens bevatten. Dit is een verplicht veld.
- <CN:value> is de algemene naam. Dit is de volledig gekwalificeerde domeinnaam (FQDN) die de exacte locatie van de server in het Domain Name System (DNS) specificeert. Dit is een verplicht veld.
- [OU:<value>] is de naam van de organisatorische eenheid of afdeling. Bijvoorbeeld Support, IT, Engineer, Finance. Dit is een optioneel veld.
- [O:<value>] is de naam van de organisatie of het bedrijf. Meestal de wettelijk erkende naam van een bedrijf. Dit is een optioneel veld.
- [ST:<value>] is de provincie, de regio, het district of de staat. Bijvoorbeeld Buckinghamshire California. Dit is een optioneel veld.
- [C:<waarde>] is het land. De tweeletterige ISO-code (International Organization for Standardization) voor het land waar uw organisatie is gevestigd. Bijvoorbeeld VS, GB, FR. Dit is een optioneel veld.
- [subjectAltName:<waarde>] is de alternatieve naam van het onderwerp (SAN). Vanaf X509, versie 3 (RFC 2459), zijn SSL-certificaten (Secure Socket Layers) toegestaan om meerdere namen op te geven die moeten overeenkomen met het certificaat. In dit veld kan het gegenereerde certificaat meerdere domeinen bestrijken. Het kan IP adressen, domeinnamen, e-mailadressen, regelmatige DNS hostnames, enz. bevatten, gescheiden door komma's. Als het wordt gespecificeerd, moet u ook de GN in deze lijst omvatten. Hoewel dit een optioneel veld is, moet het SAN-veld worden ingevuld zodat XMPP-clients (Extensible Messaging and Presence Protocol) een certificaat kunnen aanvaarden, anders wordt in de XMPP-clients een certificaatfout weergegeven.

Stap 2. Genereer callbridge, xmpp, webadmin en webbridge CSR.

1. Open de CMS CLI met Putty en Log in met de admin-account.
2. Voer de volgende opdrachten uit om CSR te maken voor elke service die op CMS nodig is. Het is ook acceptabel om één cert te maken met een wild card (*.com) of het cluster FQDN als CN, FQDN’s van elke CMS-server en, indien nodig, bij URL te voegen.

Service	opdracht
Webadmin	pki csr <cert name> CN:<server FQDN>
Webbridge	pki csr <cert name> CN:<Server FQDN> subjectAltName:<Join Url>,<XMPP domain>
callbridge OMKEREN Taakverdeling	pki csr <cert name> CN:<Server FQDN's>

3. Als het CMS geclusterd is, voert u de volgende opdrachten uit.

Service	Opdracht
callbridge OMKEREN Taakverdeling	pki csr <cert name> CN:<cluster FQDN> subjectAltName:<Peer FQDN's>
XMPP	pki csr <cert name> CN:<Cluster FQDN> subjectAltName:<XMPP Domain>,<Peer FQDN's>

Stap 3. Genereer het databasecluster CSR en gebruik ingebouwde CA om ze te ondertekenen.

Sinds CMS 2.7 moet u beschikken over certificaten voor uw databasecluster. In 2.7 hebben we een ingebouwde CA opgenomen die kan worden gebruikt om de databasecertificaten te ondertekenen.

1. Op alle kernen rennen database cluster remove.

- Op de Primaire, lopen pki selfsigned dbca CN. Voorbeeld: **Pki selfsigned dbca CN:tplab.local**
- Op Primair, looppas pki csr dbserver CN:cmscore1.example.com subjectAltName. Voorbeeld: cmscore2.example.com,cmscore3.example.com
- Maak op de Primary een cert voor database client pki csr dbclient CN:postgres .

- Gebruik op de Primaire pagina dbca om de dbserver cert **pki sign dbserver dbca** te ondertekenen.

- Op Primair, gebruik dbca om dbclient cert te ondertekenen pki sign dbclient dbca.

- Kopieer de dbclient.crt naar alle servers die verbinding moeten maken met een database knooppunt

- Kopieert het bestand dbserver.crt naar alle servers die zijn aangesloten op de database (knooppunten waaruit het databasecluster bestaat).

- Kopieer het bestand dbca.crt naar alle servers.

- Op de Primaire DB-server, run database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt. Dit gebruikt het dbca.crt als de root ca-cert .

- Voer op de primaire DB-server database cluster localnode a uit .

- Voer op de primaire DB-server database cluster initialize uit .

- Op de primaire DB-server, uitvoeren database cluster status . Moet zien knooppunten: (me): Connected Primary.

- Op alle andere kernen die zijn aangesloten bij het databasecluster, start u database cluster certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt .

- Op alle kernen die zijn aangesloten (niet op dezelfde locatie als een database) op het databasecluster, voert u de volgende handelingen uit **database cluster certs dbclient.key cbclient.crt dbca.crt** .

- Op kernen die aangesloten zijn (op dezelfde locatie als een database):

    - voer uit. database cluster localnode a

        - voer uit.database cluster join

- ON-kernen die zijn aangesloten (niet op dezelfde locatie als een database):

    - ru n database cluster localnode a .

        - voer uit. database cluster connect

Stap 4. Controleer de ondertekende certificaten.

- De geldigheid van het certificaat (vervaldatum) kan worden geverifieerd met de inspectie van het certificaat, voer de opdracht uit **pki inspect <filename>** .

    - U kunt bevestigen dat een certificaat een privé sleutel aanpast, het bevel in werking stellen pki match <keyfile> <certificate file>.

    - Om te valideren dat een certificaat is ondertekend door de CA en dat de certificaatbundel kan worden gebruikt om dit te bevestigen, voert u de opdracht pki verify <cert> <certificate bundle/Root CA> uit .

Stap 5. Ondertekende certificaten toepassen op componenten op CMS-servers.

1. Voer de volgende opdrachten uit om certificaten op Webadmin toe te passen:

```
webadmin disable
webadmin certs <keyfile> <certificate file> <certificate bundle/Root CA>
webadmin enable
```

2. Voer de volgende opdrachten uit om certificaten op CallBridge toe te passen:

```
callbridge certs <keyfile> <certificate file> <certificate bundle/Root CA>
callbridge restart
```

3. Voer de volgende opdrachten uit om certificaten op Webbridge toe te passen:

```
webbridge disable
```

```
webbridge certs <keyfile> <certificate file> <certificate bundle/Root CA>
webbridge enable
```

4. Als u certificaten op XMPP wilt toepassen, voert u de volgende opdrachten uit:

```
xmpp disable
xmpp certs <keyfile> <certificate file> <certificate bundle/Root CA>
xmpp enable
```

5. Als u certificaten op de database wilt toepassen of verlopen certificaten op het huidige DB-cluster wilt vervangen, voert u de volgende opdrachten uit:

```
database cluster remove (on all servers, noting who was primary before beginning)
database cluster certs <server_key> <server_certificate> <client_key> <client_certificate> <Root ca_crt
database cluster initialize     (only on primary node)
database cluster join <FQDN or IP of primary>    (only on slave node)
database cluster connect <FQDN or IP of primary> (only on nodes that are not part of the database clust
```

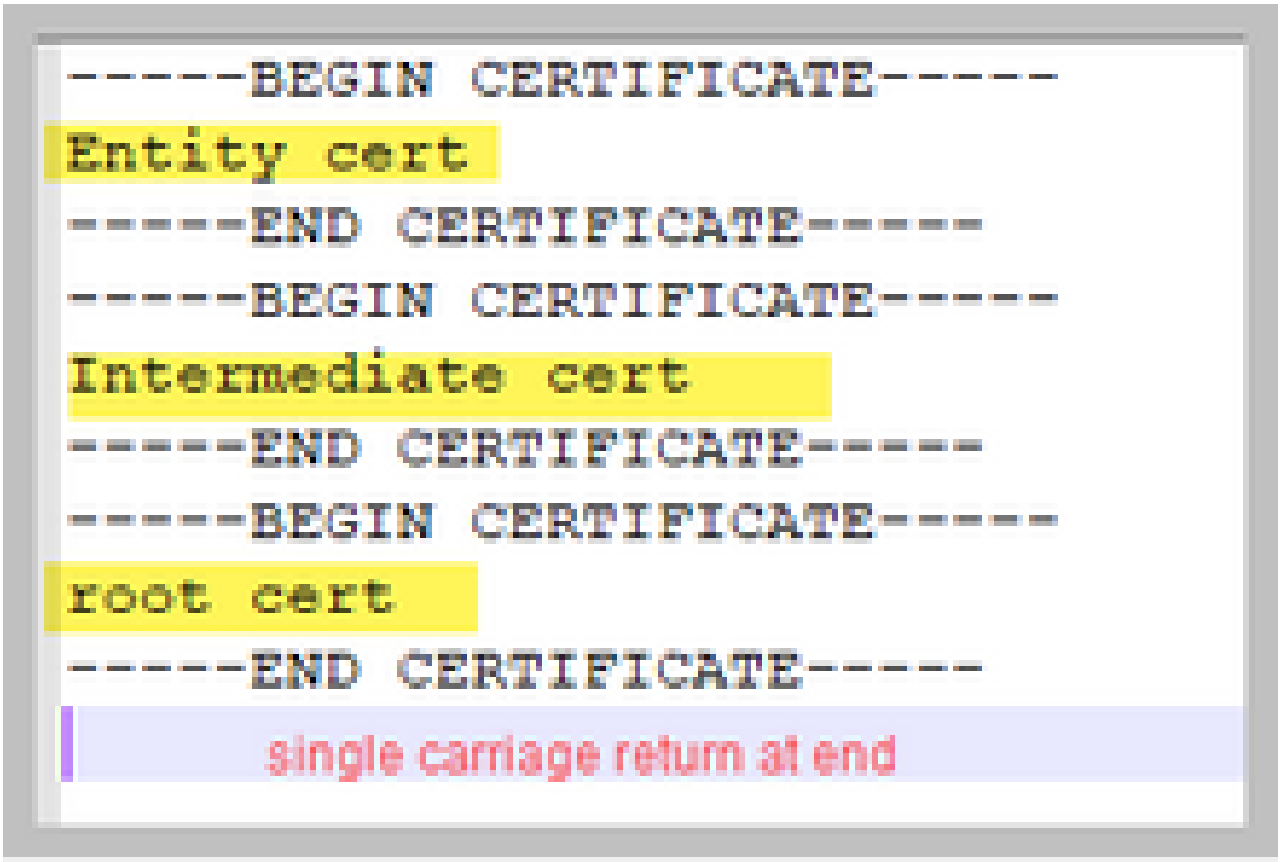
6. Voer de volgende opdrachten uit om certificaten toe te passen op turn:

```
turn disable
turn certs <keyfile> <certificate file> <certificate bundle/Root CA>
turn enable
```

Certificaat vertrouwensketens en -bundels

Sinds CMS 3.0 moet u gebruik maken van Certificate trust ketens of full chain trusts. Ook is het belangrijk voor elke dienst dat je herkent hoe certs moeten worden gebouwd wanneer je bundels maakt.

Wanneer u een certificaat vertrouwensketen, zoals vereist voor Web bridge 3, moet u het bouwen zoals getoond in het beeld, met entiteit cert bovenop, en tussenpersonen in het midden, en wortel CA onderaan, dan een enkele wagenterugloop.



Telkens als u een bundel maakt, moet het certificaat slechts één wagenterugloop aan het eind hebben.

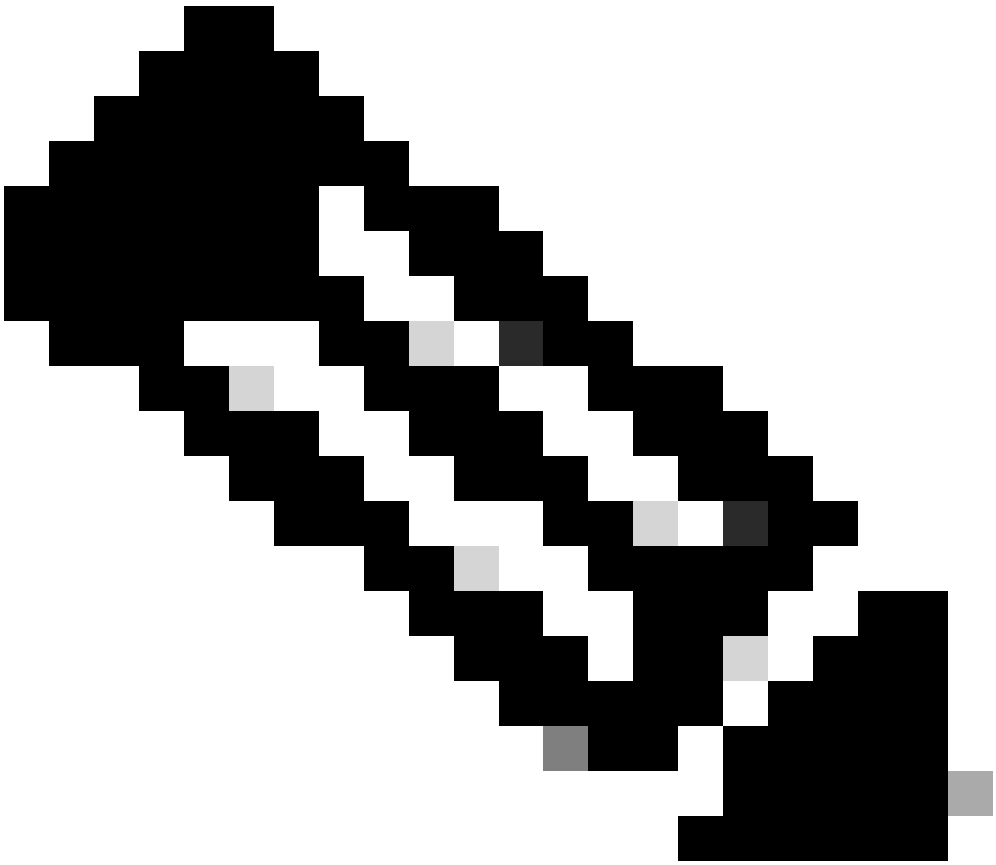
CA-bundels zouden hetzelfde zijn als getoond in de afbeelding, maar er zou natuurlijk geen entiteitscertificaat zijn.

Problemen oplossen

Als u een verlopen certificaat moet vervangen voor alle services, behalve databasecertificaten, is de eenvoudigste methode om nieuwe certs te uploaden met dezelfde naam als de oude certificaten. Als u dit doet, hoeft de service alleen opnieuw opgestart te worden en hoeft u de service niet opnieuw te configureren.

Als u presteert pki csr ... en die bepaalde naam overeenkomt met een huidige sleutel, breekt het onmiddellijk de dienst. Als de productie live is en u proactief een nieuwe CSR en Key maakt, gebruik een nieuwe naam. U kunt de naam van de momenteel actieve naam wijzigen voordat u de nieuwe cert naar de servers uploadt.

Als de database certificaten zijn verlopen, moet u controleren met **database cluster status** wie de database Primary is, en op alle knooppunten, voer de opdracht database cluster remove. Dan kunt u de instructies van Stap 3 gebruiken. Genereert het databasecluster CSR en gebruikt ingebouwde CA om ze te ondertekenen**.**



Opmerking: Raadpleeg de volgende video voor het geval u de Cisco Meeting Manager (CMM)-certificaten wilt verlengen: het Cisco Meeting Management SSL-certificaat bijwerken

---

Gerelateerde informatie

- **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.