Meervoudige adressen configureren in SAN-certificaat in CVOS-systemen

Inhoud

Inleiding

In dit document wordt beschreven hoe u een Cisco Voice Operating System (VOS)-systeem kunt instellen om meerdere adressen in het veld Subjective Alternative Name (SAN) te hebben, als de Cisco VOS-omgeving geen Publisher - Subscriber Architecture-model heeft, zoals Virtual Voice Browser (VVB).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Door CA ondertekende certificaten
- Zelfondertekende certificaten
- Cisco VOS CLI

Gebruikte componenten

- VVB
- Cisco VOS-systeembeheer - certificaatbeheer
- Cisco VOS CLI

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 configuratie wordt uitgevoerd door de Cisco VOS-opdrachtregelinterface. Dit helpt de organisatie om de webpaginaâ€™s te gebruiken en te bladeren met de hostname of Fully Qualified Domain Name (FQDN) via het beveiligde communicatiekanaal. Hierdoor rapporteert de browser geen onbetrouwbare HTTP verbinding.

Configureren

Zorg ervoor dat deze services up en functioneel zijn voordat u deze configuratie probeert uit te voeren.

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

Configuraties

Stap 1. Meld u aan bij VVB OS CLI met referenties.

Stap 2. U moet eerst de certificaatinformatie instellen voordat u MVO genereert.

- Voer de `set web-security` commando op de VVB CLI interface.

```
set web-security <orgunit> <orgname> <locality> <state> [country] [alternatehostname1,alternatehostname2
```

Voorbeeld, `set web-security tac cisco bangalore karnataka IN vvbpri,vvbpri.raducce.com` zoals in deze afbeelding.

```
admin:set web-security tac cisco bangalore karnataka IN vvbpri,vvbpri.raducce.com
```

Web security opdracht instellen

Vervolgens wordt u gevraagd te antwoorden met `Yes/No` zoals aangetoond in dit beeld.

```
WARNING: This operation creates self-signed certificate for web access (tomcat) with the updated organizational information.  However, certific
c, CallManager, CAPF, etc.) still contain the original information. You may need to re-generate these self-signed certificates to update them.

Regenerating web security certificates please wait ...

WARNING: This operation will overwrite any CA signed certificate previously imported for  tomcat
Proceed with regeneration (yes|no)?
```

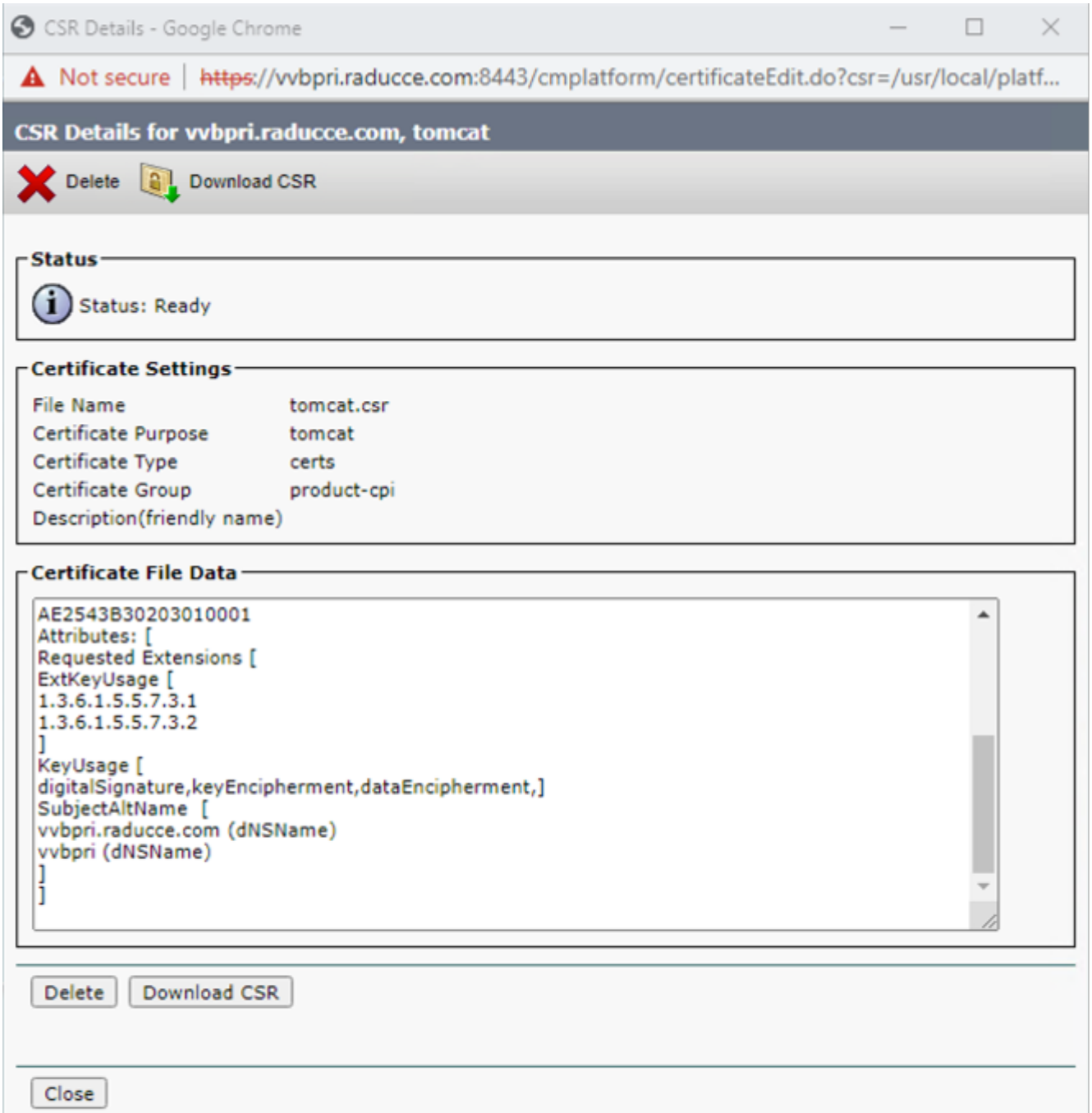
opdrachtuitvoering voor webbeveiliging instellen

- Voer in Yes
- Start de Cisco Tomcat-service opnieuw op de Cisco VOS-knooppunt.

```
utils service restart Cisco Tomcat
```

Stap 3. Genereert Tomcat-certificaatondertekeningsaanvraag (CSR) via CLI. Het commando set csr gen tomcat genereert een Tomcat-certificaat via de VOS CLI-interface.

Stap 4. Controleer op de VVB OS ADMIN certificaatbeheerpagina, een Tomcat CSR certificaat wordt gegenereerd. Klik op de Download CSR optie zoals in deze afbeelding.



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.