

Configurer plusieurs adresses dans un certificat SAN dans des systèmes CVOS

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Configurations](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer un système Cisco VOS (Voice Operating System) pour qu'il ait plusieurs adresses dans le champ de certificat Autre nom de l'objet (SAN) lorsque l'environnement Cisco VOS n'a pas de modèle d'architecture Éditeur - Abonné, par exemple Virtual Voice Browser (VVB).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Certificats signés par une autorité de certification
- Certificats auto-signés
- CLI Cisco VOS

Composants utilisés

- VVB
- Administration système Cisco VOS - Gestion des certificats
- CLI Cisco VOS

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La configuration est effectuée via l'interface de ligne de commande Cisco VOS. Cela permet à l'entreprise d'utiliser et de parcourir les pages Web avec le nom d'hôte ou le nom de domaine complet (FQDN) via le canal de communication sécurisé. Par conséquent, le navigateur ne signale pas de connexion HTTP non approuvée.

Configurer

Avant d'essayer cette configuration, assurez-vous que ces services sont opérationnels ;

- Service Cisco Tomcat
- Notification de changement de certificat Cisco
- Cisco Certificate Expiry Monitor

Configurations

Étape 1. Connectez-vous à VVB OS CLI avec les informations d'identification.

Étape 2. Vous devez d'abord définir les informations de certificat avant la génération de CSR.

- Exécutez la commande `set web-security` sur l'interface CLI VVB.

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

Exemple : `set web-security tac cisco bangalore karnataka IN vvbpri,vvbpri.raducce.com` comme le montre cette image.



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

Commande Set web-security

Ensuite, il vous invite à répondre avec Yes/No comme le montre cette image.

```
WARNING: This operation creates self-signed certificate for web access (tomcat) with the updated organizational information. However, certificates (e.g., 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]? █
```

set web-security, commande exécution

- Saisissez `Yes`
- Redémarrez le service Cisco Tomcat sur le noeud Cisco VOS.

```
utils service restart Cisco Tomcat
```

Étape 3. Générez une demande de signature de certificat (CSR) Tomcat via l'interface de ligne de commande. La commande `set csr gen tomcat` génère un certificat Tomcat à partir de l'interface CLI de VOS.

Étape 4. Vérifiez sur la page de gestion des certificats ADMIN du système d'exploitation VVB qu'un certificat CSR Tomcat est généré. Cliquez sur le bouton `Download CSR` comme illustré dans cette image.

CSR Details - Google Chrome

Not secure | <https://vvpri.raducce.com:8443/cmplatform/certificateEdit.do?csr=/usr/local/platf...>

CSR Details for vvpri.raducce.com, tomcat

Delete Download CSR

Status

Status: Ready

Certificate Settings

File Name	tomcat.csr
Certificate Purpose	tomcat
Certificate Type	certs
Certificate Group	product-cpi
Description(friendly name)	

Certificate File Data

```
AE2543B30203010001
Attributes: [
Requested Extensions [
ExtKeyUsage [
1.3.6.1.5.5.7.3.1
1.3.6.1.5.5.7.3.2
]
KeyUsage [
digitalSignature,keyEncipherment,dataEncipherment,]
SubjectAltName [
vvpri.raducce.com (dNSName)
vvpri (dNSName)
]
]
```

Delete Download CSR

Close

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.