Konfigurieren mehrerer Adressen im SAN-Zertifikat in CVOS-Systemen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie ein Cisco Voice Operating System (VOS)-System so einrichten, dass mehrere Adressen im Feld "Subject Alternative Name (SAN)"-Zertifikat angezeigt werden, wenn die Cisco VOS-Umgebung kein Publisher/Subscriber-Architekturmodell aufweist, z. B. Virtual Voice Browser (VVB).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- CA-signierte Zertifikate
- Selbstsignierte Zertifikate
- Cisco VOS-CLI

Verwendete Komponenten

- VVB
- Cisco VOS-Systemverwaltung - Zertifikatsverwaltung
- Cisco VOS-CLI

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die Konfiguration wird über die Cisco VOS-Befehlszeilenschnittstelle durchgeführt. Dies hilft dem Unternehmen, die Webseiten entweder mit dem Hostnamen oder mit dem vollqualifizierten Domänennamen (FQDN) über den sicheren Kommunikationskanal zu verwenden und zu durchsuchen. Dadurch meldet der

Browser keine nicht vertrauenswürdige HTTP-Verbindung.

Konfigurieren

Stellen Sie vor der Konfiguration sicher, dass diese Services betriebsbereit und funktionsfähig sind.

- Cisco Tomcat Service
- Benachrichtigung über Änderung des Cisco Zertifikats
- Überwachung auf Ablauf von Cisco Zertifikaten

Konfigurationen

Schritt 1: Melden Sie sich mit Anmeldeinformationen bei der VB-BS-CLI an.

Schritt 2: Sie müssen die Zertifikatinformationen vor der Erstellung der CSR-Anfrage festlegen.

- Führen Sie die `set web-security` -Befehls auf der VVB-CLI-Schnittstelle ein.

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

Beispiele, `set web-security tac cisco bangalore karnataka IN vvbpri,vvbpri.raducce.com` wie in diesem Bild dargestellt.

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

Websicherheitsbefehl festlegen

Als Nächstes werden Sie aufgefordert, mit Yes/No wie in diesem Bild gezeigt.

```
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)?
```

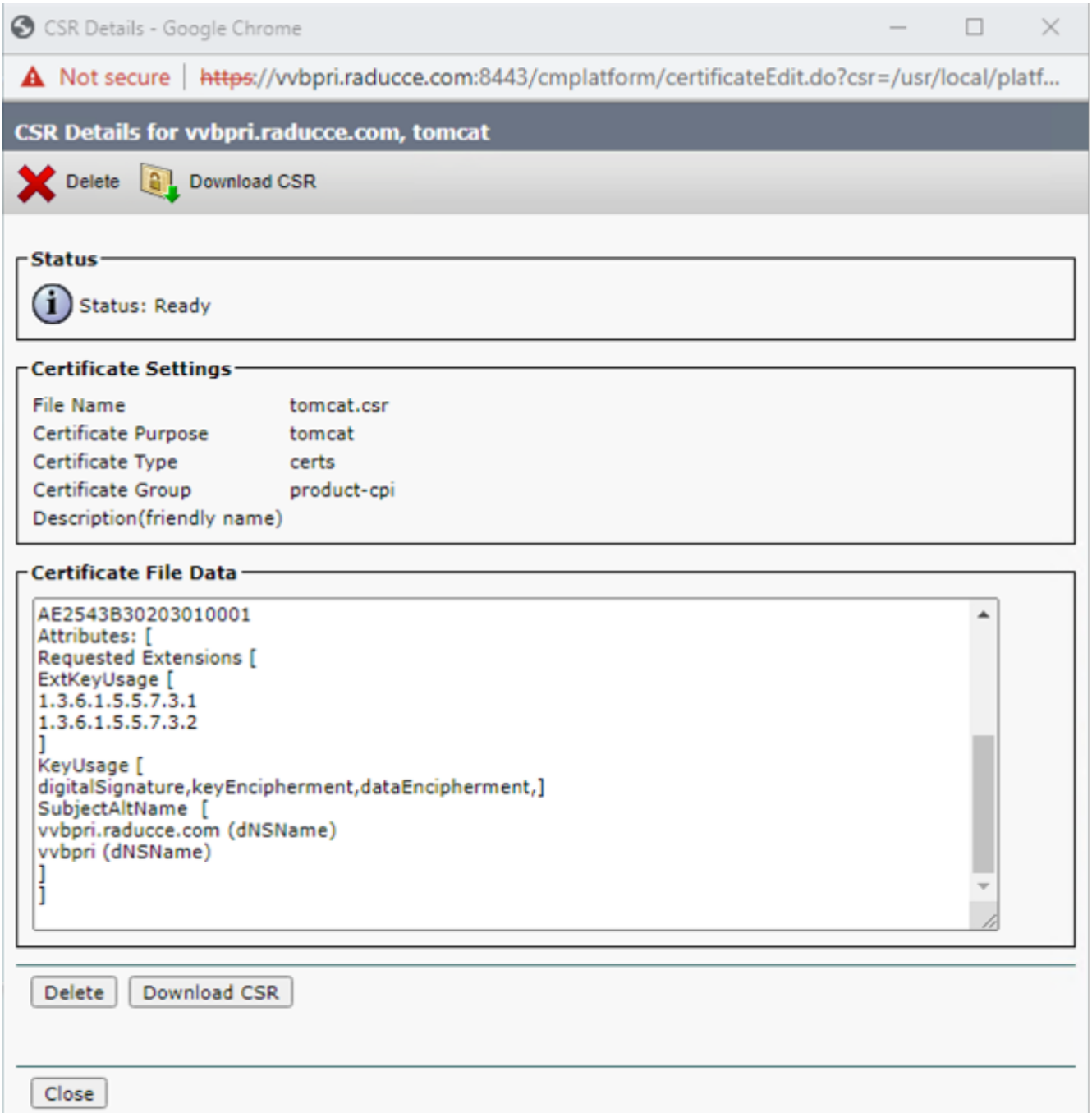
Ausführen des Befehls set web-security

- Eingabe Yes
- Starten Sie den Cisco Tomcat-Dienst auf dem Cisco VOS-Knoten neu.

```
utils service restart Cisco Tomcat
```

Schritt 3: Generieren einer Tomcat-Zertifikatsignierungsanforderung (CSR) über CLI Der Befehl set csr gen tomcat generiert ein Tomcat-Zertifikat über die VOS-CLI-Schnittstelle.

Schritt 4: Überprüfen Sie auf der Verwaltungsseite für das VVB OS ADMIN-Zertifikat, ob ein Tomcat CSR-Zertifikat generiert wurde. Klicken Sie auf Download CSR wie in diesem Bild dargestellt.



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.