CVOSシステムでのSAN証明書の複数のアドレスの設定

内容

概要

このドキュメントでは、Cisco VOS環境にVirtual Voice Browser(VVB)などのパブリッシャ – サブスクライバアーキテクチャモデルがない場合に、Subject Alternative Name(SAN)証明書フィールドに複数のアドレスを持つようにCisco Voice Operating System(VOS)システムを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CA署名付き証明書
- 自己署名証明書
- Cisco VOSのCLI

使用するコンポーネント

- VVB
- Cisco VOS System Administration：証明書管理
- Cisco VOSのCLI

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

設定は、Cisco VOSのコマンドラインインターフェイスを介して伝送されます。これにより、組織はホスト名または完全修飾ドメイン名(FQDN)を使用して、セキュアな通信チャネルを介してWebページを使用し、閲覧できます。これにより、ブラウザは信頼できないHTTP接続を報告しません。

設定

この設定を開始する前に、次のサービスが稼働していることを確認してください。

- Cisco Tomcat サービス
- Cisco Certificate Change Notification
- Cisco証明書の有効期限の監視

コンフィギュレーション

ステップ 1： クレデンシャルを使用してVVB OS CLIにログインします。

ステップ 2：CSRを生成する前に、最初に証明書情報を設定する必要があります。

- を実行します。 set web-security コマンドをVVB CLIインターフェイスで発行します。

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

たとえば、 set web-security tac cisco bangalore karnataka IN vvbpri,vvbpri.raducce.com 以下の図に、出力例を示します。

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

Set web-securityコマンド

次に、応答を求めるプロンプトが表示されます。 Yes/No 次の図に示すようにします。

```
WARNING: This operation creates self-signed certificate for web access (tomcat) with the updated organizational information.  However, certificates for other components (ipse
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)?
```

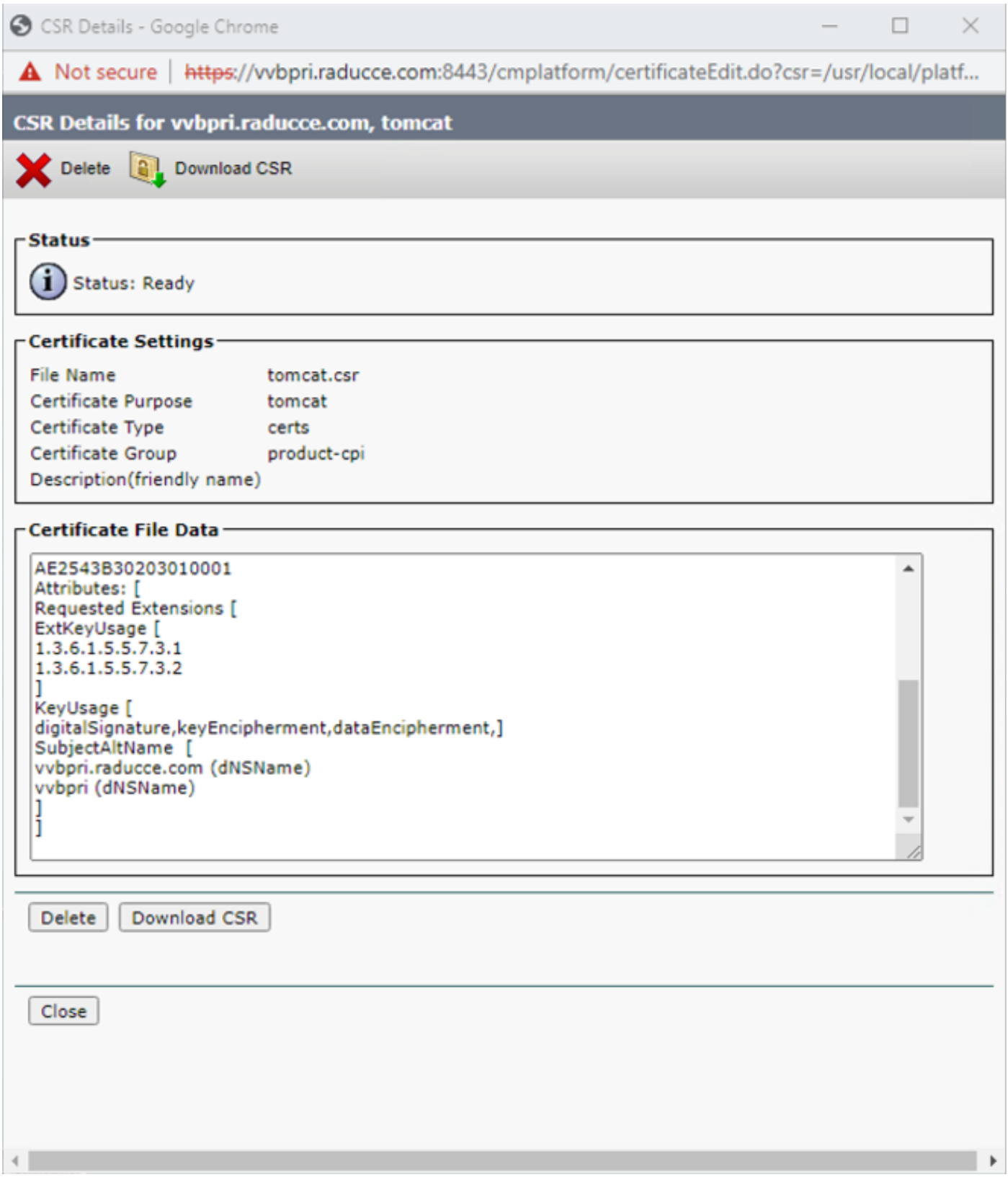
set web-securityコマンドの実行

- Yes
- Cisco VOSノードでCisco Tomcatサービスを再起動します。

```
utils service restart Cisco Tomcat
```

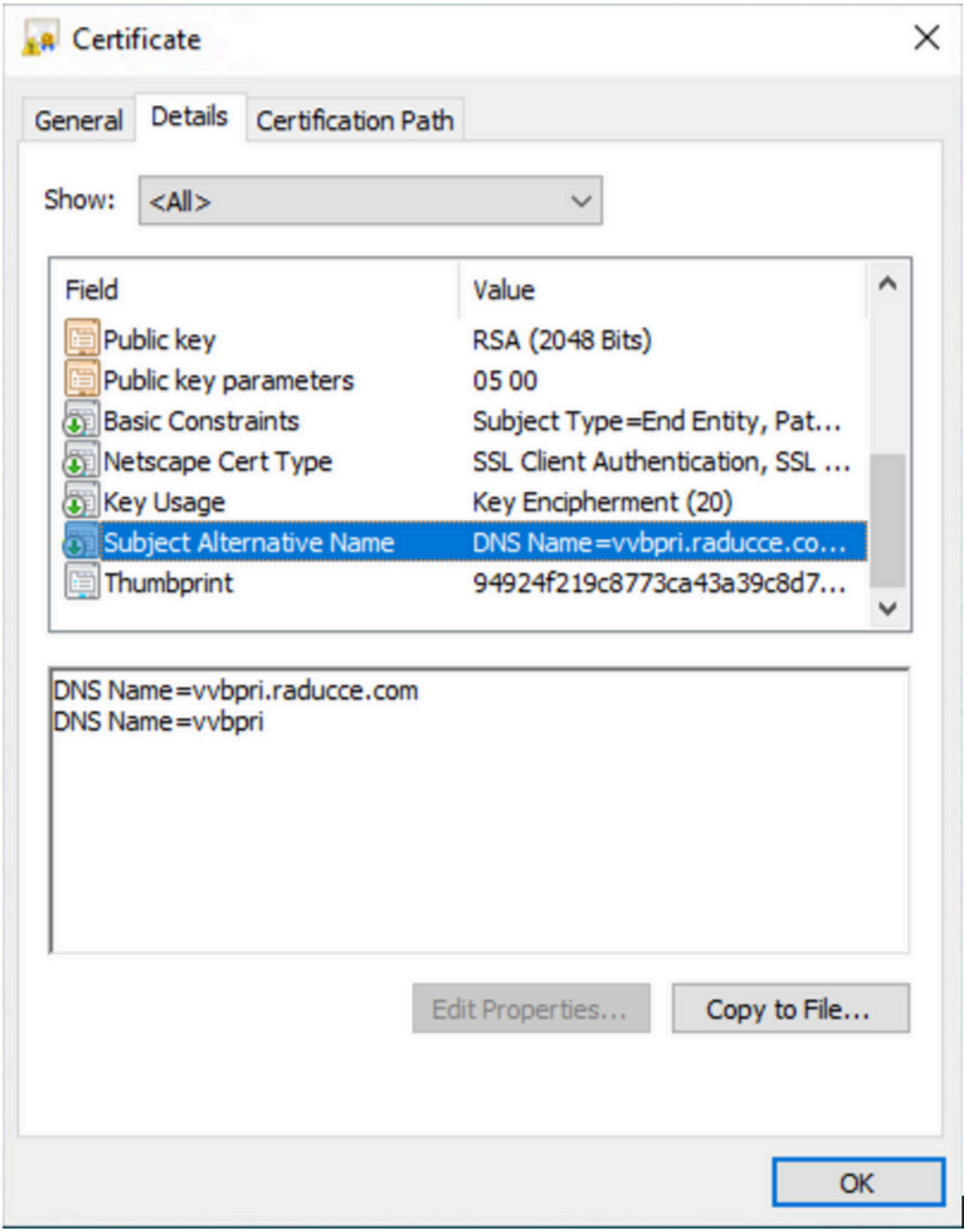
ステップ 3：CLIを使用してTomcat証明書署名要求(CSR)を生成します。 `set csr gen tomcat` VOS CLIインターフェイスからTomcat証明書を生成します。

ステップ 4：VVB OS ADMIN証明書管理ページで、Tomcat CSR証明書が生成されることを確認します。をクリックします。 Download CSR オプションを選択します。



ステップ 5：CAチームにCSR証明書を提供し、CAによって署名された証明書を取得します。

手順 6：この図では、SAN内のCA where-inによって署名された証明書は、前述のコマンドで設定された複数のアドレスを示しています。



Tomcat CA署名付き証明書

確認

ここでは、設定が正常に機能しているかどうかを確認します。

1. にログインします VOS Portal URL ページで、 LOCK アイコンをクリックし、SAN証明書フィールドで定義されているアドレスを確認します。
2. SANフィールドで定義されたアドレスを使用して、セキュアなHTTP通信を確認します。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

CLIアクセスから次の証明書管理ログを収集し、Cisco TACでケースをオープンします。 file get activelog platform/log/cert*

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。