Cisco 音声 オペレーティング システム（VOS）の CLI による設定 CA 署名入り認証

目次

概要

この資料は方法のコンフィギュレーションのステップを Command Line Interface （CLI）の使用によってあらゆる Cisco 音声 オペレーティング システム（VOS）基づいた Collaboration Server のサード パーティ 認証局（CA） 署名入り認証をアップ ロードする記述したものです。

前提条件

要件

次の項目に関する知識が推奨されます。

- Public Key Infrastructure（PKI）および実装 on Cisco VOS サーバおよび Microsoft CA の基本的な知識
- DNS インフラストラクチャは前もって構成されます

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- VOS サーバ: Cisco Unified Communications Manager （ CUCM ）バージョン 9.1.2
- CA： Windows 2012 サーバ
- クライアント ブラウザ: Mozilla Firefox バージョン 47.0.1

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

Comunications すべての Cisco Unified VOS 製品では少なくとも 2 つの資格情報型があります: アプリケーションは（ccmadmin、ccmservice、cuadmin、cfadmin、cuic）好みましたりおよび VOS （cmplatform、drf、cli）プラットフォーム。

いくつかの特定のシナリオでアプリケーションを Webページによって管理し、コマンド・ラインによってプラットフォーム関連アクティビティを行うことは非常に便利です。 あなたの下で CLI によってサード パーティ 署名入り認証をもっぱらインポートする方法のプロシージャを見つけるかもしれないです。 この Tomcat 例で証明書はアップ ロードされます。 CallManager か他のどのアプリケーションに関してはそれは同じを検知 します。

生成する CA 署名入り認証

サマリ コマンド

技術情報で使用されるコマンドのリスト。

```
show cert list own
show cert own tomcat

set csr gen CallManager
show csr list own
show csr own CallManager

show cert list trust
set cert import trust CallManager
set cert import own CallManager CallManager-trust/allevich-DC12-CA.pem
```

正しい証明書情報をチェックして下さい

すべてのアップ ロードされた信頼できる証明書をリストして下さい。

```
admin:show cert list own

tomcat/tomcat.pem: Self-signed certificate generated by system
ipsec/ipsec.pem: Self-signed certificate generated by system
CallManager/CallManager.pem: Certificate Signed by allevich-DC12-CA
CAPF/CAPF.pem: Self-signed certificate generated by system
TVS/TVS.pem: Self-signed certificate generated by system
```

だれが Tomcat サービスのための証明書を発行したかチェックして下さい。

```
admin:show cert own tomcat

[
  Version: V3
  Serial Number: 859978324705545211023663245198594366 90
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: L=Krakow, ST=Malopolskie, CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, C=PL
  Validity From: Sun Jul 31 11:37:17 CEST 2016
           To:   Fri Jul 30 11:37:16 CEST 2021
  Subject Name: L=Krakow, ST=Malopolskie, CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, C=PL
  Key: RSA (1.2.840.113549.1.1.1)
    Key value: 3082010a0282010100a2
<output omited>
```

これは発行元がサブジェクトと一致するので自己署名証明書です。

生成する 証明書 サイン 要求 (CSR)

生成する CSR。

```
admin:set csr gen tomcat
Successfully Generated CSR  for tomcat
```

証明書 サイン requst が正常に生成されたことを確認して下さい。

```
admin:show csr list own
tomcat/tomcat.csr
```

それを開き、テキストファイルにコンテンツをコピーして下さい。 それをように tac_tomcat.csr ファイル保存して下さい。

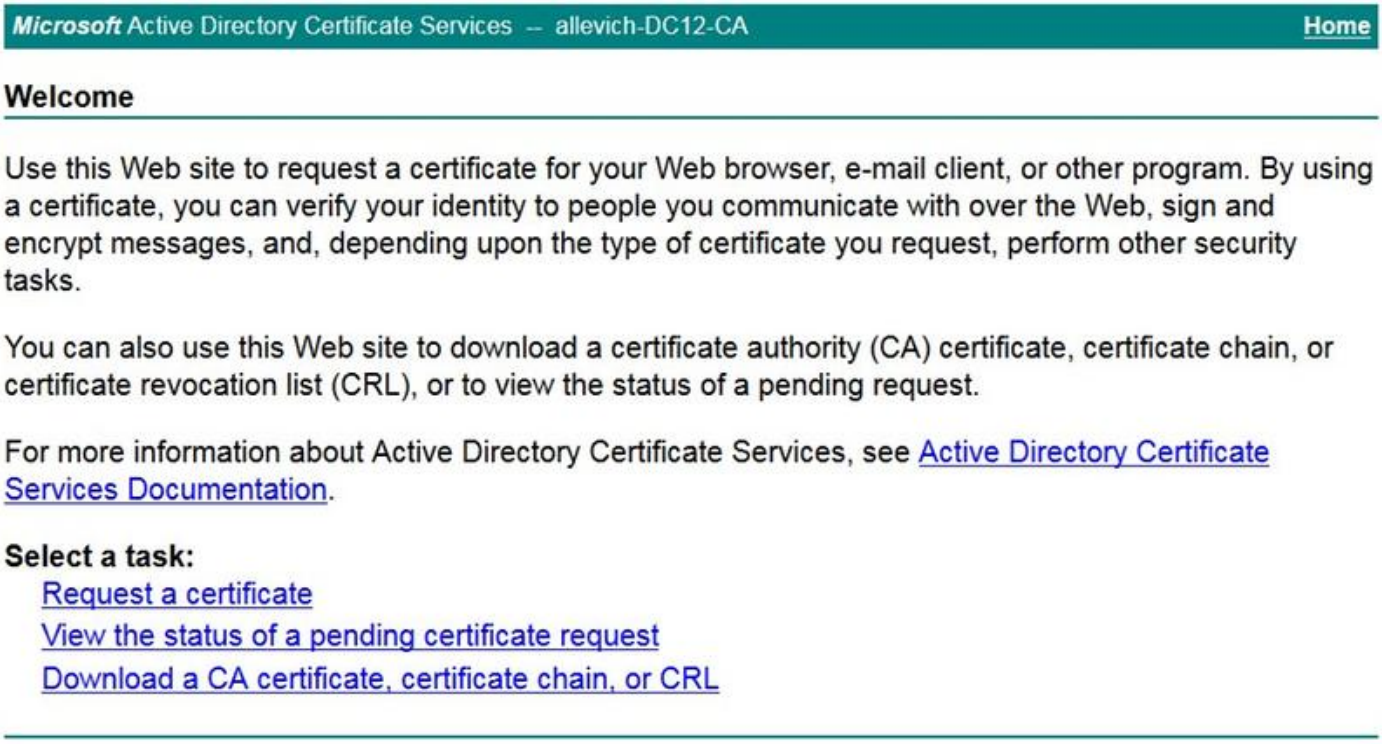
```
admin:show csr own tomcat

-----BEGIN CERTIFICATE REQUEST-----
MIIDSjCCAjICAQAwgb0xCzAJBgNVBAYTAlBMMRQwEgYDVQQIEwtNYWxvcG9sc2tp
ZTEPMA0GA1UEBxMGS3Jha293MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFD
MR4wHAYDVQQDExV1Y20xLTEuYWxsZXZpY2gubG9jYWwxSTBHBgNVBAUTQDlhMWJk
NDA5M2VjOGYxNjljODhmNGUyZTYwZTYzM2RjNjlhZmFkNDY1YTgzMDhkNjRhNGU1
MzExOGQ0YjZkZjcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCVo5jh
lMqTUnYbHQUnYPt00PTflWbj7hi6PSYI7pVCbGUZBpIZ5PKwTD56OZ8SgpjYX5Pf
l9D09H2gtQJTMVv1Gm1eGdlJsbuABRKn6lWkO6b706MiGSgqel+41vnItjn3Y3kU
7h51nruJye3HpPQzvXXpOKJ/JeJc8InEvQcC/UQmFMKn0ulO0veFBHnG7TLDwDaQ
W1Al1rwrezN9Lwn2a/XZQR1P65sjmnkFFF2/FON4BmooeiiNJD0G+F4bKig1ymlR
84faF27plwHjcw8WAn2HwJT6O7TaE6EOJd0sgLU+HFAI3txKycS0NvLuMZYQH81s
/C74CIRWibEWT2qLAgMBAAGgRzBFBgkqhkiG9w0BCQ4xODA2MCcGA1UdJQQgMB4G
CCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAwUwCwYDVR0PBAQDAgO4MA0GCSqG
SIb3DQEBBQUAA4IBAQBUu1FhKuyQ1X58A6+7KPkYsWtioS0PoycltuQsVo0aav82
PiJkCvzWTeEo6v9qG0nnaI53e15+RPpWxpEgAIPPhtt6asDuW30SqSx4eClfgmKH
ak/tTuWmZbfyk2iqNFy0YgYTeBkG3AqPwWUCNoduPZ0/fo41QoJPwjE184U64WXB
gCzhIHfsV5DzYp3IR5C13hEa5fDgpD2ubQWja2LId85NGHEiqyiWqwmt07pTkBc+
7ZKa6fKnpACehrtVqEn02jOi+sanfQKGQqH8VYMFsW2uYFj9pf/Wn4aDGuJoqdOH
StV2Eh0afxPEq/1rQP3/rzq4NMYlJ7glyNFGPUVP
-----END CERTIFICATE REQUEST-----
```

Tomcat サーバ証明を生成して下さい

CA で Tomcat サービスのための証明書を生成して下さい。

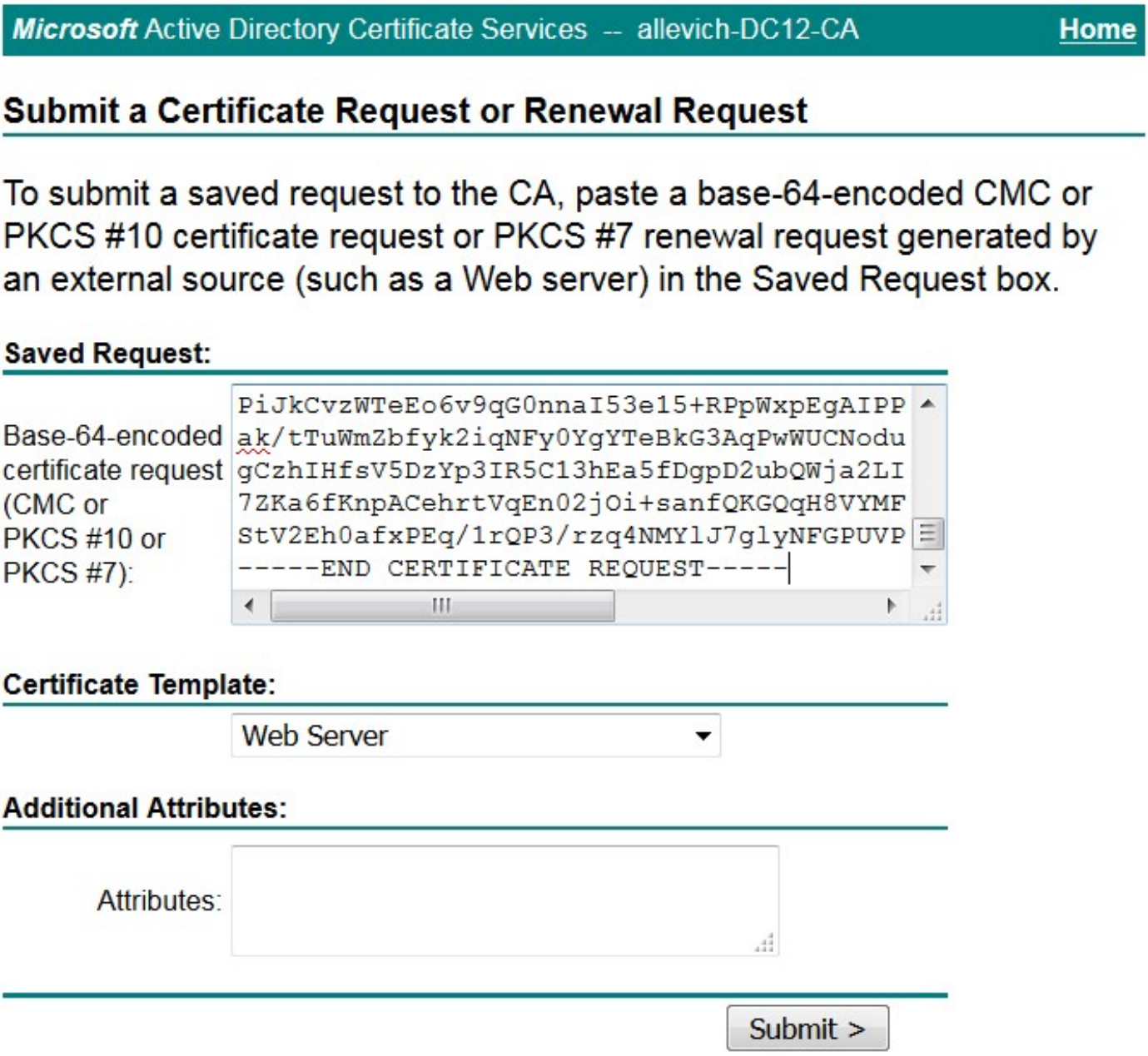
ブラウザののための Webページを認証局（CA）開いて下さい。 認証プロンプトに正しい資格情報を置いて下さい。

http://dc12.allevich.local/certsrv/



CA ルート証明をダウンロードして下さい。 メニューを『Download a CA certificate， certificate chain， or CRL』 を選択 して下さい。 Next メニューでリストから適切な CA を選択して下さい。 符号化 方式は **Base 64** であるはずです。 CA 認証をダウンロードし、ネーム **ca.cer** のオペレーティング システムにそれを保存して下さい。

Certificate 要求を『Request a certificate』 を押し、次に**進めました。 証明書のテンプレートを** Webサーバに設定 し、示されている**ように**テキストファイル **tac_tomcat.csr** からの CSR コンテンツを貼り付けて下さい。



ヒント： オペレーションがラボで (行われればまたは Cisco VOS サーバおよび CA は時間を節約する同じ管理ドメインの下に) コピー アンド ペーストしますメモリバッファからの CSR をあります。

『SUBMIT』 を押して下さい。 オプションを『Base 64 encoded』 を選択 し、Tomcat サービスのための証明書をダウンロードして下さい。

注: 証明書 生成がバルクで meaninful 1 に証明書の名前を変更するために実行された確認して下さい。

Cisco VOS サーバに Tomcat 証明書をインポートして下さい

CA 認証をインポートして下さい

CA 認証を開いて下さいネーム **ca.cer** と保存された。 それは最初にインポートする必要がありま

す。

コンテンツをバッファにコピーし、CUCM CLI の次のコマンドを入力して下さい:

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

CA 認証を貼り付けるプロンプトは表示する。 下記に示されているようにそれを貼り付けて下さい。

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

信頼できる証明書アップ ロードが正常ならこの出力は表示する。

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

CA 認証が Tomcat 信頼 1 として正常にインポートされることを確認して下さい。

```
admin:show cert list trust

tomcat-trust/ucm1-1.pem: Trust Certificate
tomcat-trust/allevich-win-CA.pem: w2008r2 139
<output omited for brevity>
```

Tomcat 証明書をインポートして下さい

次のステップは Tomcat CA 署名入り認証をインポートすることです。 オペレーションは Tomcat

信頼証明書と同様に、ちょうどコマンドが異なっている同じを検知 します。

```
set cert import own tomcat tomcat-trust/allevich-DC12-CA.pem
```

サービスを再起動する

そして最後に Tomcat サービスを再開して下さい。

```
utils service restart Cisco Tomcat
```

> **注意**： それがエクステンションモビリティ、不在着信、社内 ディレクトリおよび他のような Webサーバ依存したサービスのオペレーションを、中断することに留意して下さい。

確認

生成された証明書を確認して下さい。

```
admin:show cert own tomcat

[
  Version: V3
  Serial Number: 276529240473076562022540660071542142548731496 5
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: CN=allevich-DC12-CA, DC=allevich, DC=local
  Validity From: Sun Jul 31 12:17:46 CEST 2016
           To:   Tue Jul 31 12:17:46 CEST 2018
  Subject Name: CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL
  Key: RSA (1.2.840.113549.1.1.1)
    Key value: 3082010a028201010095a
```

発行人名がその証明書を組み立てた CA に属するようにして下さい。

ブラウザのサーバの FQDN をタイプすることによって Webページにログインすれば証明書警告は表示する。

トラブルシューティング

この記事の目的は公開キー Infrastucture （ PKI ）の論理を強調表示しないために CLI によって証明書をアップ ロードする方法のコマンド構文のプロシージャを与えることです。 それは SAN 証明書、従属 CA、4096 Certificate 鍵 長さおよび他の多くのシナリオをカバーしません。

Webサーバ 証明書を CLI によってアップ ロードした場合オペレーションが CA 認証」を読むことが不可能なエラーメッセージと「失敗するまれに。 それのための対応策は Webページを使用して証明書をインストールすることです。

非標準認証局（ CA ） 設定は認証インストールにおける問題を引き起こす原因となる場合があります。 基本的なデフォルト 設定を用いる別の CA から証明書を生成し、インストールすることを試みて下さい。

計画はキャンセルします

自己署名証明書を生成する必要性があればまた CLI ですることができます。

下記のコマンドをタイプすれば Tomcat 証明書は自己署名ものに再生します。

```
admin:set cert regen tomcat

WARNING: This operation will overwrite any CA signed certificate previously imported for  tomcat

Proceed with regeneration (yes|no)? yes
Successfully Regenerated Certificate for tomcat.

You must restart services related to tomcat for the regenerated certificates to become active.
```

新しい証明書 Tomcat サービスを適用することは再起動する必要があります。

```
admin:utils service restart Cisco Tomcat

 Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted
Properly, execute the same Command Again

Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Commanded Out of Service
Cisco Tomcat[NOTRUNNING]
Service Manager is running
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
```

関連記事

Webページによるアップ ロード証明書

得るべきプロシージャおよび署名する Upload ウィンドウ サーバ 自己-または認証局（CA）…