Configurez le certificat signé CA par l'intermédiaire du CLI dans le système d'exploitation de Voix de Cisco (VOS)

Contenu

Introduction

Ce document décrit des étapes de configuration sur la façon dont télécharger le certificat signé d'Autorité de certification (CA) de tiers sur n'importe quel serveur basé de Collaboration du système d'exploitation de Voix de Cisco (VOS) à l'aide de l'interface de ligne de commande (CLI).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base d'Infrastructure à clés publiques (PKI) et son implémentation sur les serveurs et le Microsoft CA de Cisco VOS
- L'infrastructure de DN est préconfigurée

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Serveur VOS : Version 9.1.2 de Cisco Unified Communications Manager (CUCM)
- CA : Serveur de Windows 2012
- Navigateur de client : Version 47.0.1 de Mozilla Firefox

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Dans des tous les Produits de Cisco Unified Comunications VOS il y a au moins deux types de qualifications : l'application aiment (ccmadmin, ccmservice, cuadmin, cfadmin, cuic) et des plates-formes VOS (cmplatform, drf, cli).

Dans quelques scénarios spécifiques il est très commode de gérer des applications par l'intermédiaire de la page Web et d'exercer des activités relatives par plate-forme par l'intermédiaire de la ligne de commande. Au-dessous de vous peut trouver une procédure sur la façon dont importer le certificat signé de tiers seulement par l'intermédiaire du CLI. Dans ce Tomcat d'exemple le certificat est téléchargé. Pour le CallManager ou n'importe quelle autre application il regarde la même chose.

Générez le certificat signé CA

Commandes récapitulatives

Une liste des commandes utilisées dans l'article.

```
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
```

Les informations correctes de certificat de contrôle

Répertoriez tous les Certificats de confiance téléchargés.

```
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
```

Vérifiez qui a délivré le certificat pour le service de Tomcat.

```
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>
```

C'est un certificat auto-signé puisque l'émetteur apparie le sujet.

Générez la demande de signe de certificat (le CSR)

Générez le CSR.

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

Vérifiez que le requst de signe de certificat a été généré avec succès.

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

Ouvrez-le et copiez le contenu sur le fichier texte. Sauvegardez-le comme **fichier tac_tomcat.csr**.

```
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
```

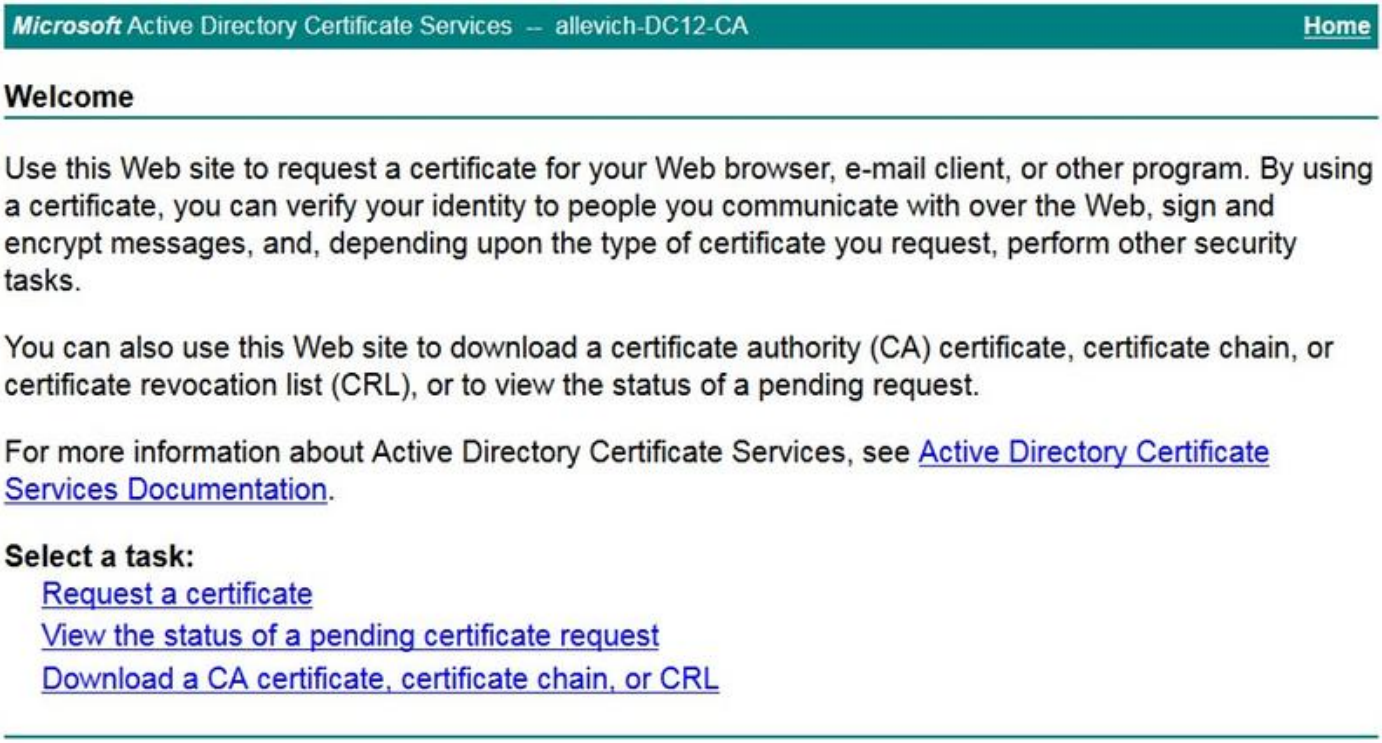
```
StV2Eh0afxPEq/1rQP3/rzq4NMYlJ7glyNFGPUVP
-----END CERTIFICATE REQUEST-----
```

Générez le certificat de serveur de Tomcat

Générez un certificat pour le service de Tomcat sur le CA.

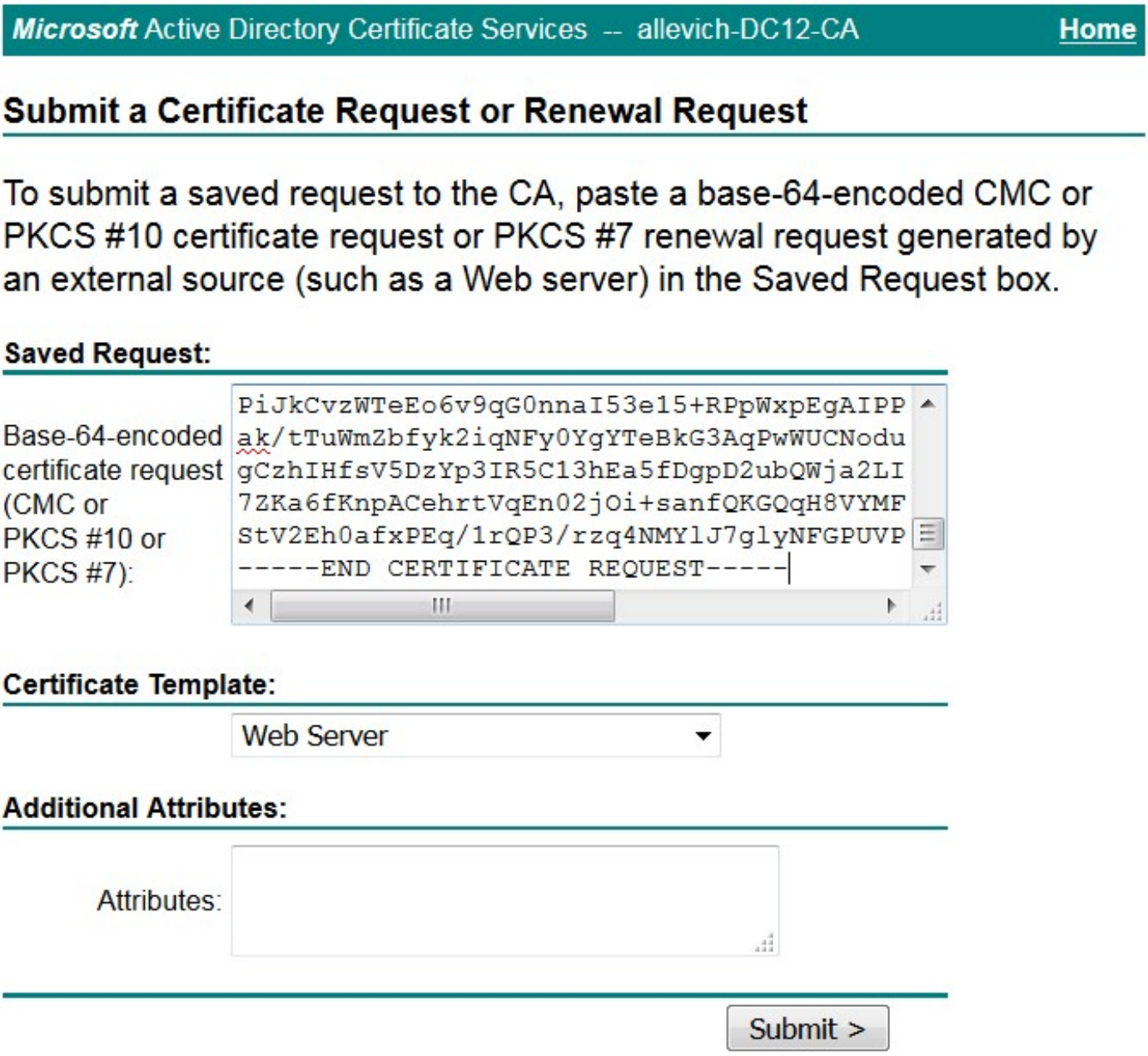
Ouvrez la page Web pour l'autorité de certification dans un navigateur. Mettez les qualifications correctes dans la demande d'authentification.

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



Téléchargez le certificat racine CA. Sélectionnez le **téléchargement un certificat de CA, une chaîne de certificat, ou un** menu **CRL**. Dans le prochain menu choisissez le CA approprié de la liste. La méthode de codage devrait être la **base 64**. Téléchargez le certificat de CA et sauvegardez-le au système d'exploitation avec le nom **ca.cer**.

Appuyez sur la **demande un certificat** et une **demande** alors **avancée de certificat**. Placez le **modèle de certificat au** web server et collez le contenu CSR à partir du fichier texte **tac_tomcat.csr comme** affiché.



> **Conseil** : Si l'exécution est faite dans le laboratoire (ou le serveur de Cisco VOS et le CA est sous le même domaine administratif) pour sauvegarder la copie de temps et pour coller le CSR du tampon mémoire.

La presse **soumettent**. L'option **encodée de la base 64** choisis et téléchargent le certificat pour le service de Tomcat.

> **Note**: Si la génération de certificat est exécutée en vrac assurez pour changer un nom du certificat à meaninful.

Certificat de Tomcat d'importation au serveur de Cisco VOS

Certificat de CA d'importation

Ouvrez le certificat de CA qui a été enregistré avec un nom **ca.cer**. Il doit être importé d'abord.

Copiez son contenu sur la mémoire tampon et introduisez la commande suivante dans le CUCM CLI :

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

La demande pour coller le certificat de CA sera affichée. Collez-le comme affiché ci-dessous.

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

Au cas où un téléchargement de certificat de confiance serait réussi cette sortie sera affichée.

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

Vérifiez que le certificat de CA est avec succès importé comme Tomcat-confiance une.

```
admin:show cert list trust

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

Certificat de Tomcat d'importation

L'étape suivante est d'importer le certificat signé de Tomcat CA. L'exécution regarde les mêmes qu'avec le CERT de Tomcat-confiance, juste la commande est différente.

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

Redémarrez le service

Et redémarrez pour finir le service de Tomcat.

```
utils service restart Cisco Tomcat
```

> **Attention** : Maintenez dans l'esprit qu'il perturbe l'exploitation des services dépendants de web server, comme la mobilité d'extension, les appels manqués, le répertoire d'entreprise et les autres.

Vérifiez

Vérifiez le certificat qui a été généré.

```
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
```

Assurez-vous que le nom d'émetteur appartient au CA qui a construit ce certificat.

La procédure de connexion à la page Web en tapant le FQDN du serveur dans un navigateur et aucun avertissement de certificat sera affichée.

Dépanner

Le but de cet article est de donner une procédure avec la syntaxe de commande sur la façon dont télécharger le certificat par l'intermédiaire du CLI, pour ne pas mettre en valeur la logique de la clé publique Infrastucture (PKI). Il ne couvre pas le certificat SAN, le CA subalterne, la longueur principale de 4096 certificats et beaucoup d'autres scénarios.

Dans des quelques rares cas en téléchargeant un certificat de web server par l'intermédiaire du CLI l'exécution échoue avec un message d'erreur « incapable de lire le certificat de CA ». Un contournement pour celui est d'installer le certificat utilisant la page Web.

Une configuration non standard d'autorité de certification peut mener au problème avec l'installation de certificat. Essayez de générer et installer le certificat d'un autre CA avec une configuration par défaut de base.

Soutiennent le plan

Au cas où il y aura un besoin de générer un certificat auto-signé il peut également être fait dans le CLI.

Introduisez la commande ci-dessous et le certificat de Tomcat sera régénéré à auto-signé.

```
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.
```

Pour appliquer un nouveau service de Tomcat de certificat doit être redémarrée.

```
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]
```

Articles relatifs

[Certificat de téléchargement par l'intermédiaire de page Web]

[Procédure pour obtenir et télécharger le - d'individu de Windows Server signé ou l'Autorité de certification (CA)…]