Contenu

Introduction

Ce document décrit comment identifier si le certificat signé d'Autorité de certification (CA) apparie la demande de signature de certificat existant (CSR) des serveurs d'applications de Cisco Unified.

Conditions préalables

Conditions requises

Reccommends de Cisco que vous avez la connaissance de X.509/CSR.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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

Une demande de certification se compose d'un nom unique, d'une clé publique, et d'un ensemble facultatif d'attributs, collectivement signé par l'entité demandant la certification. Des demandes de certification sont envoyées à une autorité de certification qui transforme la demande en certificat de clé publique X.509. Dans quel formulaire l'autorité de certification renvoie le certificat nouvellement signé est hors de portée de ce document. Un message PKCS #7 est un possibility.(RFC:2986)

Gestion de certificat de Cisco Communications Manager

L'intention d'inclure un ensemble d'attributs est double :

- Pour fournir d'autres informations sur une entité donnée, ou un mot de passe de défi par lequel l'entité peut plus tard demander la révocation de certificat.
- Pour fournir des attributs pour l'intégration dans les Certificats X.509. Les serveurs UC de courant ne prennent en charge pas un mot de passe de défi.

Les serveurs en cours de Cisco UC ont besoin de ces attributs dans un CSR suivant les indications de cette table :

Les informations	Description
orgunit	unité organisationnelle
orgname	nom organisationnel
localité	emplacement d'organisation
état	état d'organisation
pays	code de pays ne peut pas être changé
alternatehostname	nom d'hôte alternatif

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified IM et présence
- Unity Connection de Cisco Unified
- CUIS
- Cisco Meidasence
- Cisco Unified Contact Center Express (UCCX)

Problème

En prenant en charge l'UC, vous rencontrez beaucoup de cas où le CA certificat signé ne le télécharge pas sur les serveurs UC. Vous ne pouvez pas toujours identifier ce qui s'est produit pendant la création du certificat signé, puisque vous n'êtes pas la personne qui a utilisé le CSR pour créer le certificat signé. Dans la plupart des scénarios, la re-signature d'un nouveau certificat prend plus de 24 heures. Les serveurs UC tels que CUCM n'ont pas détaillé le log/suivi pour aider à identifier pourquoi le téléchargement de certificat échoue mais ils donnent juste un message d'erreur. Cet article est destiné pour aider au rétrécissement en bas de la question, si c'est un serveur UC ou une question CA.

Pratique générale pour les Certificats Ca-signés dans CUCM

CUCM prend en charge l'intégration avec la tierce partie CAs à l'aide d'un mécanisme CSR PKCS#10 qui est accessible au GUI du système d'exploitation de gestionnaire de certificat de Cisco Unified Communications. Les clients, qui utilisent actuellement la tierce partie CAs doivent employer le mécanisme CSR pour délivrer des Certificats pour le Cisco CallManager, le CAPF, l'IPSec, et le Tomcat.

Étape 1. Changez l'identifier avant de générer le CSR

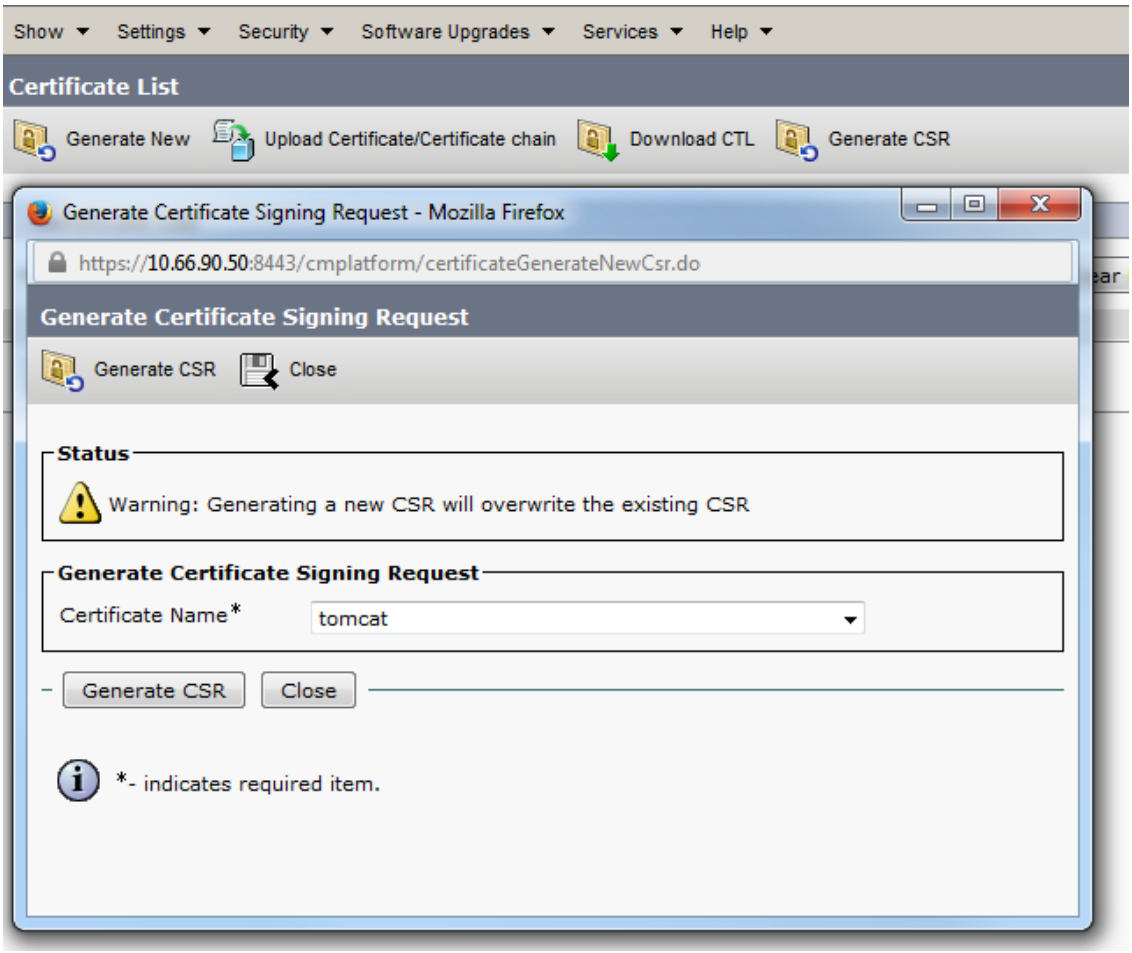
L'identité du serveur CUCM pour générer un CSR peut être modifiée à l'aide de la **sécurité Web réglée de** commande suivant les indications de cette image.

```
admin:set web-security  ?
Syntax:
set web-security orgunit orgname locality state [country] [alternatehostname]
orgunit  mandatory   organizational unit
orgname  mandatory   organizational name
locality mandatory   location of organization
state    mandatory   state of organization
country  optional    country code can not be changed
alternatehostname  optional   alternate host name

admin:set web-security
```

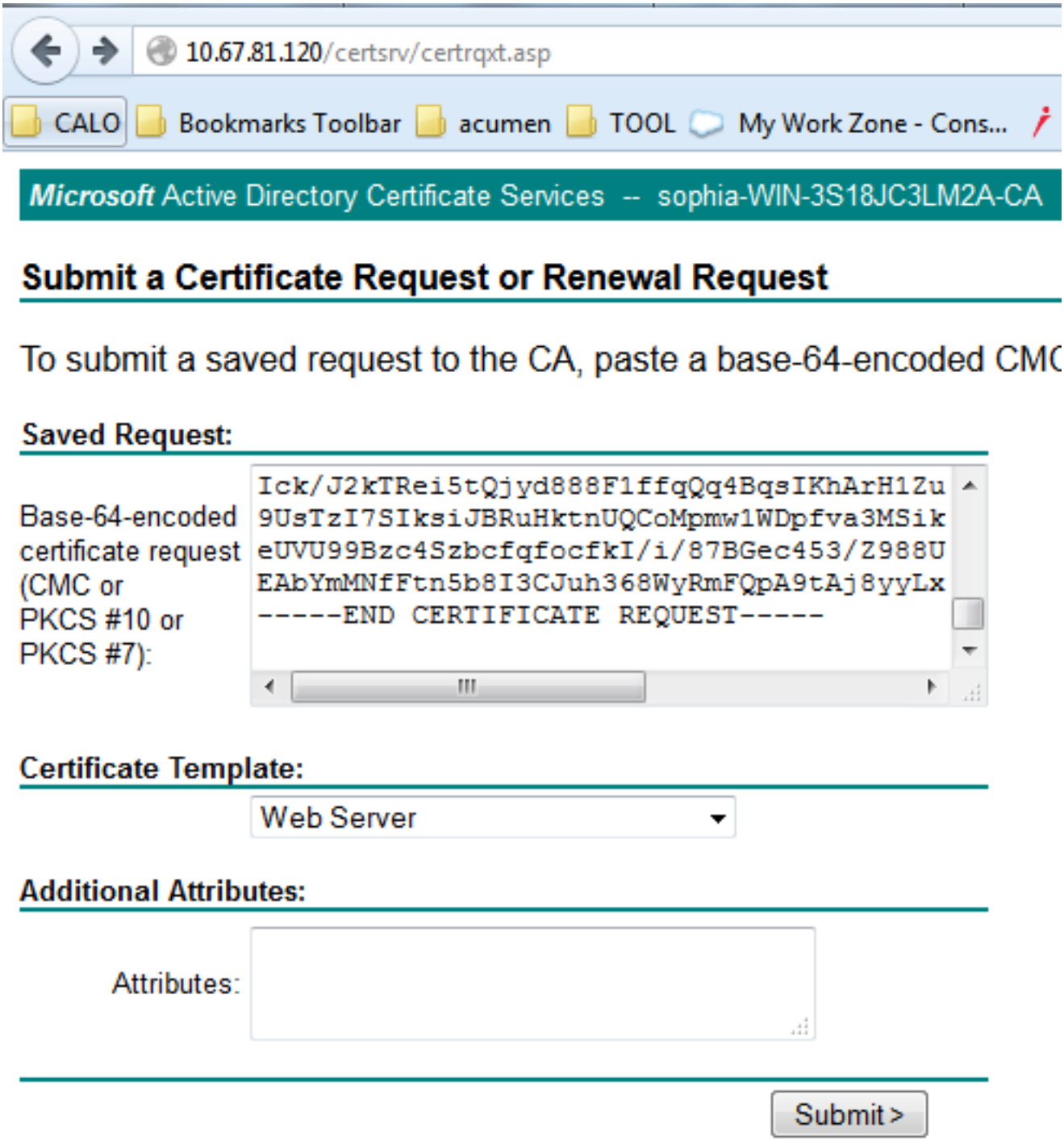
Si vous avez l'espace dans les domaines ci-dessus, l'utilisez s'il vous plaît ? ? pour réaliser la commande en tant que :

```
admin:set web-security "Cisco Systems" "Cisco TAC" "St Leonard" NSW AU CUCM105.sophia.li

WARNING: Country code can not be changed.
Country code for existing web-security is : AU

WARNING: This operation creates self signed certificate for web access (tomcat) with the
r, certificates for other components (ipsec, callmanager, CAPF, etc.) still contain the o
erate 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
Proceed with regeneration (yes|no)?
```

Étape 2. Générez le CSR.

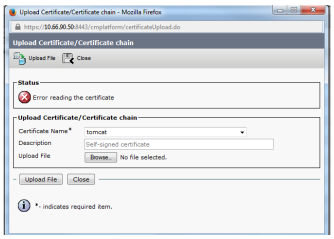


Étape 3. Téléchargez le CSR et obtenez-le a signé par le CA.



Étape 4. Téléchargez le certificat Ca-signé au serveur.

Une fois que le CSR est généré et le certificat est signé, si vous ne le téléchargez pas avec une **erreur de lecture de** message d'erreur le **certificat** (suivant les indications de cette image), alors vous devez vérifier si le CSR est régénéré ou si le certificat signé lui-même est la cause de la question.



Il y a trois manières de vérifier si le CSR est régénéré ou le certificat signé lui-même est la cause de la question.

Solution 1. Utilisez la commande d'OpenSSL dans la racine (ou le Linux)

1. Ouvrez une session à la racine et naviguez vers le répertoire.

```
[root@CCM105PUB keys]# pwd
/usr/local/platform/.security/tomcat/keys
[root@CCM105PUB keys]# ls -thl
total 28K
-rwxr-xr-x. 1 certbase ccmbase 1.7K Sep  1 23:22 tomcat_priv_csr.pem
-rwxr-xr-x. 1 certbase ccmbase 1.2K Sep  1 23:22 tomcat_priv_csr.der
-rwxr-xr-x. 1 certbase ccmbase 1.4K Sep  1 23:22 tomcat.csr
-rwxr-xr-x. 1 certbase ccmbase 1.2K Aug 13 16:11 tomcat_priv.der
-rwxr-xr-x. 1 certbase ccmbase 1.7K Aug 13 16:11 tomcat_priv.pem
-rwxr-xr-x. 1 certbase ccmbase   16 Apr 26 15:10 tomcat-trust.passphrase
-rwxr-xr-x. 1 certbase ccmbase   16 Apr 26 15:10 tomcat.passphrase
[root@CCM105PUB keys]#
```

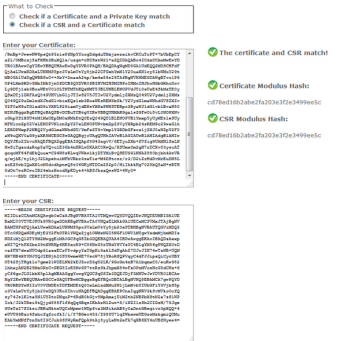
2. Copiez le certificat signé sur le même répertoire utilisant le FTP sécurisé (SFTP). Si vous ne pouvez pas installer un serveur de SFTP, alors le téléchargeant au répertoire TFTP obtient également le certificat sur le CUCM.

```
[root@CCM105PUB keys]# sftp cisco@10.66.90.19
bash: sftp: command not found
[root@CCM105PUB keys]# sftp cisco@10.66.90.19
Connecting to 10.66.90.19...
Authenticated with partial success.
cisco@10.66.90.19's password:
Hello, I'm freeFTPd 1.0sftp> get tomcat.cer
Fetching /tomcat.cer to tomcat.cer
/tomcat.cer                                   100% 2140     2.1KB/s   00:00
sftp>
```

3. Vérifiez le MD5 pour le CSR et le certificat signé.

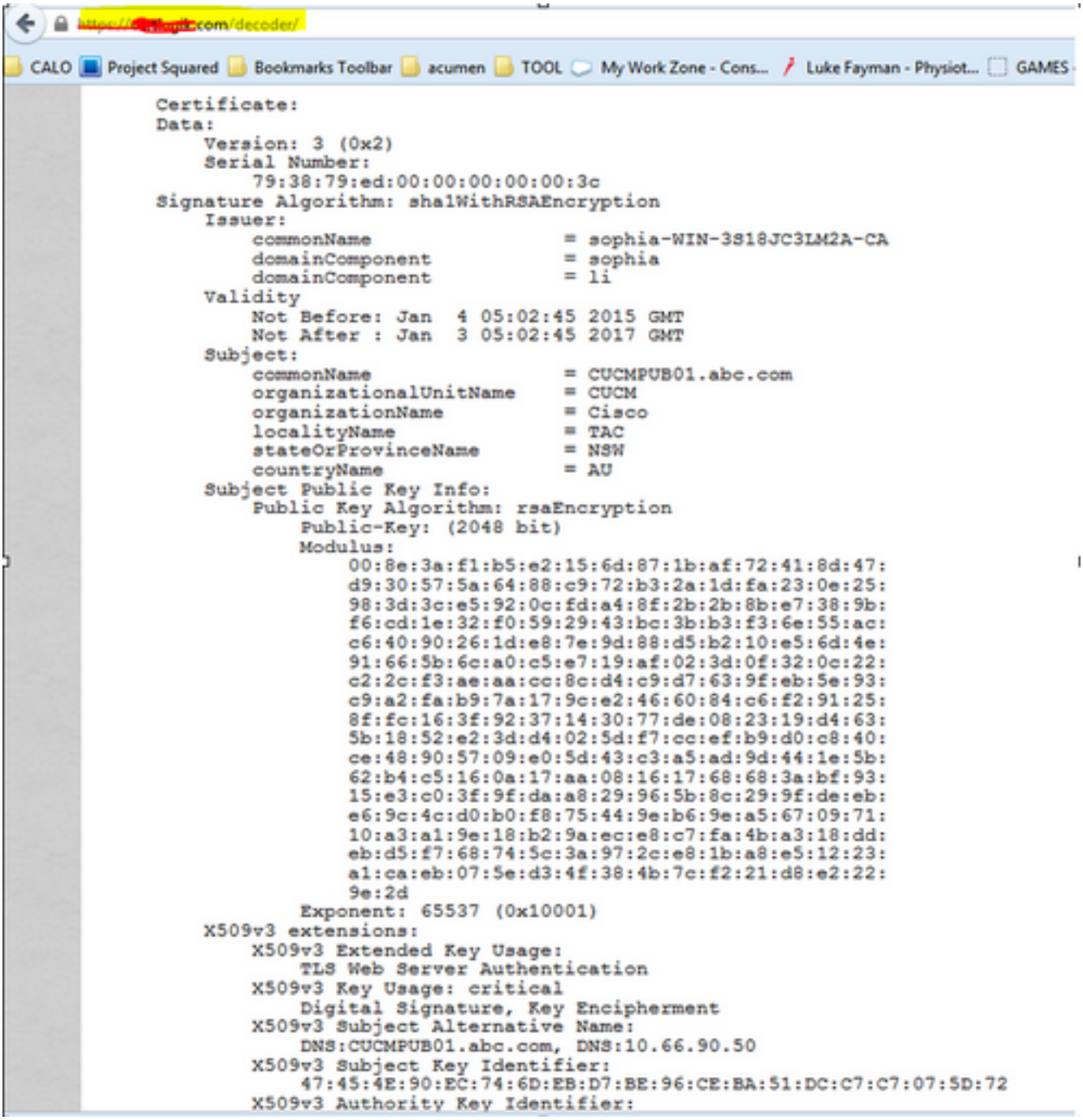
```
[root@CUCMPUB01 keys]# openssl req -noout -modulus -in tomcat.csr | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]# openssl x509 -noout -modulus -in certnew.cer | openssl md5
cd78ed16b2abe2fa203e3f2e3499ee5c
[root@CUCMPUB01 keys]#
```

Solution 2. Utilisez n'importe quelle bouveteuse de clé de certificat ssl de l'Internet



La solution 3. comparent le contenu de n'importe quel décodeur CSR de l'Internet

1. Copiez les **informations détaillées de certificat de** session pour chacun suivant les indications de cette image.



2. Comparez-les dans un outil tel que Notepad++ au module d'extension de comparer suivant les indications de cette image.