Génération de CSR et application de certificats à CMS

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Générer le CSR

- Étape 1. Structure de la syntaxe
- Étape 2 : génération du CSR Callbridge, Smpp, Webadmin et Webbridge
- Étape 3. Générer le CSR du cluster de bases de données et utiliser l'autorité de certification intégrée pour les signer
- Étape 4. Vérification des certificats signés
- Étape 5. Application des certificats signés aux composants sur les serveurs CMS

Chaînes et ensembles de certificats de confiance

Dépannage

Informations connexes

Introduction

Ce document décrit comment générer une demande de signature de certificat (CSR) et télécharger des certificats signés vers Cisco Meeting Server (CMS)

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base du serveur CMS

Composants utilisés

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

- Putty ou logiciel similaire
- CMS version 2.9 ou ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Générer le CSR

Il existe deux façons de générer un CSR : l'une consiste à générer le CSR directement sur le serveur CMS à partir de l'interface de ligne de commande (CLI) avec un accès administrateur, l'autre consiste à le faire avec une autorité de certification tierce externe, telle qu'Open SSL.

Dans les deux cas, le CSR doit être généré avec la syntaxe correcte pour que les services CMS fonctionnent correctement.

Étape 1. Structure de la syntaxe

```
pki csr <key/cert basename> <CN:value> [OU:<value>] [O:<value>] [ST:<-value>] [C:<value>] [subjectAltNa
```

- **<key/cert basename>** est une chaîne qui identifie la nouvelle clé et le nom CSR. Il peut contenir des caractères alphanumériques, des traits d'union ou des traits de soulignement. Ce champ est obligatoire.
- **<CN : value>** est le nom commun. Il s'agit du nom de domaine complet (FQDN) qui spécifie l'emplacement exact du serveur dans le système de noms de domaine (DNS). Ce champ est obligatoire.
- [OU : **<valeur>**] est le nom de l'unité organisationnelle ou du service. Par exemple, Support, informatique, Ingénieur, Finance. Ce champ est facultatif.
- [O : **<valeur>**] est le nom de l'organisation ou de l'entreprise. Il s'agit généralement du nom légalement constitué d'une société. Ce champ est facultatif.
- [ST : **<valeur>**] représente la province, la région, le comté ou l'état. Par exemple, Buckinghamshire California. Ce champ est facultatif.
- [C:**<valeur>**] est le pays. Code ISO (International Organization for Standardization) de deux lettres pour le pays dans lequel votre organisation est située. Par exemple, US, GB, FR. Ce champ est facultatif.
- [subjectAltName:**<value>**] est le nom alternatif du sujet (SAN). À partir de la version 3 de X509 (RFC 2459), les certificats SSL (Secure Socket Layers) sont autorisés à spécifier plusieurs noms auxquels le certificat doit correspondre. Ce champ permet au certificat généré de couvrir plusieurs domaines. Il peut contenir des adresses IP, des noms de domaine, des adresses e-mail, des noms d'hôte DNS standard, etc., séparés par des virgules. S'il est spécifié, vous devez également inclure le CN dans cette liste. Bien qu'il s'agisse d'un champ facultatif, le champ SAN doit être renseigné pour que les clients XMPP (Extensible Messaging and Presence Protocol) puissent accepter un certificat, sinon les clients XMPP affichent une erreur de certificat.

Étape 2 : génération du CSR Callbridge, Smpp, Webadmin et Webbridge

1. Accédez à l'interface de ligne de commande de CMS avec Putty et connectez-vous avec le

compte admin.

2. Exécutez les commandes suivantes afin de créer CSR pour chaque service requis sur CMS. Il est également acceptable de créer un certificat unique avec un caractère générique (*.com) ou avec le nom de domaine complet du cluster comme CN, les noms de domaine complets de chaque serveur CMS et l'URL de jointure si nécessaire.

Service	Commande
Webadmin	pki csr CN:
Webbridge	pki csr CN: subjectAltName: ,
Pont d'appel TOURNER Équilibreur de charge	pki csr CN:

3. Si le CMS est mis en grappe, exécutez les commandes suivantes.

Service	Commande
Pont d'appel TOURNER Équilibreur de charge	pki csr CN: subjectAltName:

XMPP	pki csr CN: subjectAltName: ,

Étape 3. Générer le CSR du cluster de bases de données et utiliser l'autorité de certification intégrée pour les signer

Depuis CMS 2.7, vous devez disposer de certificats pour votre cluster de base de données. Dans la version 2.7, nous avons inclus une autorité de certification intégrée qui peut être utilisée pour signer les certificats de base de données.

1. Sur tous les coeurs, exécutez la suppression du cluster de base de données.
2. Sur le routeur principal, exécutez pki self signed dbca CN. Exemple : Pki selfsigned dbca CN : tplab.local
3. Sur le routeur principal, exécutez pki csr dbserver CN:cmscore1.example.com subjectAltName. Exemple : cmscore2.example.com,cmscore3.example.com.
4. Sur le serveur principal, créez un certificat pour la base de données clientpki csr dbclient CN : postgres.
5. Sur le serveur principal, utilisez dbca pour signer dbserver certpki sign dbserver dbca.
6. Sur le routeur principal, utilisez dbca pour signer le certificat dbclient pki sign dbclient dbca.
7. Copiez le fichier dbclient.crt sur tous les serveurs qui doivent se connecter à un noeud de base de données
8. Copiez le fichier dbserver.crt sur tous les serveurs joints à la base de données (noeuds qui constituent le cluster de base de données).
9. Copiez le fichier dbca.crt sur tous les serveurs.
10. Sur le serveur de base de données principale, exécutez le cluster de base de données certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt. Cette commande utilise dbca.crt comme ca-cert racine.
11. Sur le serveur de base de données principale, exécutez le noeud local de cluster de base de données a.
12. Sur le serveur de base de données principale, exécutez database cluster initialize.
13. Sur le serveur de base de données principale, exécutez l'état du cluster de base de données. Noeuds à voir obligatoirement : (me) : Principal connecté.

14. Sur tous les autres coeurs qui sont joints au cluster de base de données, exécutez le cluster de base de données certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt.
15. Sur tous les coeurs connectés (non colocalisés avec une base de données) au cluster de base de données, exécutez database cluster certs dbclient.key dbclient.crt dbca.crt.
16. Sur les coeurs qui sont joints (colocalisés avec une base de données) :
    - exécutez database cluster localnode a.
    - exécuter une jointure de cluster de base de données.
17. Coeurs ON connectés (non colocalisés avec une base de données) :
    - exécuter cluster de base de données localnode a.
    - Exécuter connexion cluster base de données.

Étape 4. Vérification des certificats signés

- La validité du certificat (date d'expiration) peut être vérifiée avec l'inspection de certificat, exécutez la commande pki inspect <filename>.
- Vous pouvez valider qu'un certificat correspond à une clé privée, exécuter la commande pki match <keyfile> <certificate file>.
- Afin de valider qu'un certificat est signé par l'autorité de certification et que le groupe de certificats peut être utilisé pour l'affirmer, exécutez la commande pki verify <cert> <certificate bundle/Root CA>.

Étape 5. Application des certificats signés aux composants sur les serveurs CMS

1. Afin d'appliquer des certificats à Webadmin, exécutez les commandes suivantes :

```
webadmin disable
webadmin certs <keyfile> <certificate file> <certificate bundle/Root CA>
webadmin enable
```

2. Afin d'appliquer des certificats à Callbridge, exécutez les commandes suivantes :

```
callbridge certs <keyfile> <certificate file> <certificate bundle/Root CA>
callbridge restart
```

3. Afin d'appliquer des certificats à Webbridge, exécutez les commandes suivantes (remplacées par webbridge3 dans CMS 3.x avec les nouvelles exigences de configuration) :

```
webbridge disable
webbridge certs <keyfile> <certificate file> <certificate bundle/Root CA>
webbridge enable
```

4. Afin d'appliquer des certificats à XMPP, exécutez les commandes suivantes (Non disponible dans CMS 3.x) :

```
xmpp disable
xmpp certs <keyfile> <certificate file> <certificate bundle/Root CA>
xmpp enable
```

5. Afin d'appliquer des certificats à la base de données ou de remplacer les certificats expirés sur le cluster de base de données actuel, exécutez les commandes suivantes :

```
database cluster remove (on all servers, noting who was primary before beginning)
database cluster certs <server_key> <server_certificate> <client_key> <client_certificate> <Root ca_crt
database cluster initialize     (only on primary node)
database cluster join <FQDN or IP of primary>    (only on slave node)
database cluster connect <FQDN or IP of primary> (only on nodes that are not part of the database clust
```

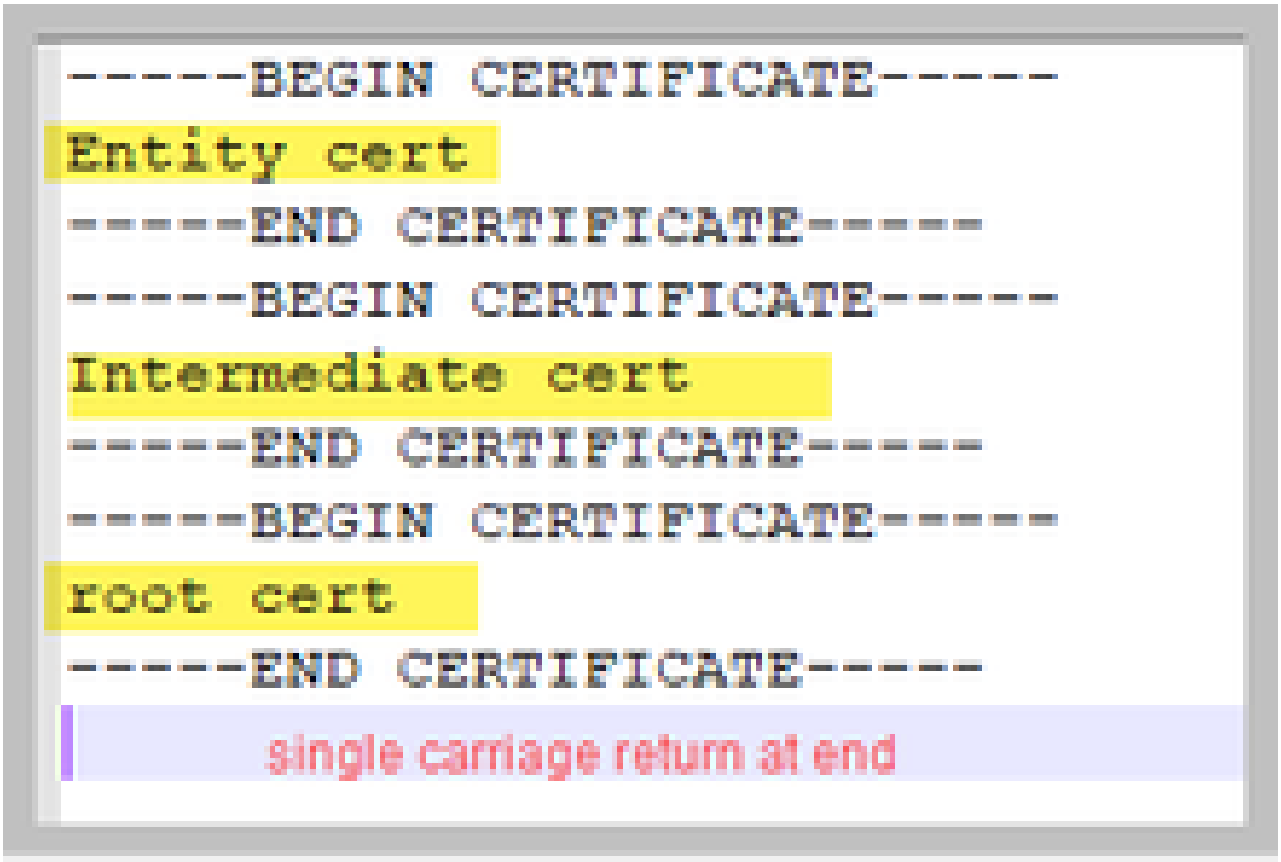
6. Afin d'appliquer des certificats à TURN, exécutez les commandes suivantes :

```
turn disable
turn certs <keyfile> <certificate file> <certificate bundle/Root CA>
turn enable
```

Chaînes et ensembles de certificats de confiance

Depuis CMS 3.0, vous devez utiliser des chaînes d'approbation de certificat ou des approbations de chaîne complète. En outre, il est important pour tout service que vous reconnaissiez comment les certificats doivent être construits lorsque vous faites des offres groupées.

Lorsque vous créez une chaîne de certificats de confiance, comme requis pour le pont Web 3, vous devez la construire comme indiqué dans l'image, avec le certificat d'entité en haut, les intermédiaires au milieu, l'autorité de certification racine en bas, puis un seul retour chariot.



Chaque fois que vous créez un lot, le certificat ne doit comporter qu'un seul retour chariot à la fin.

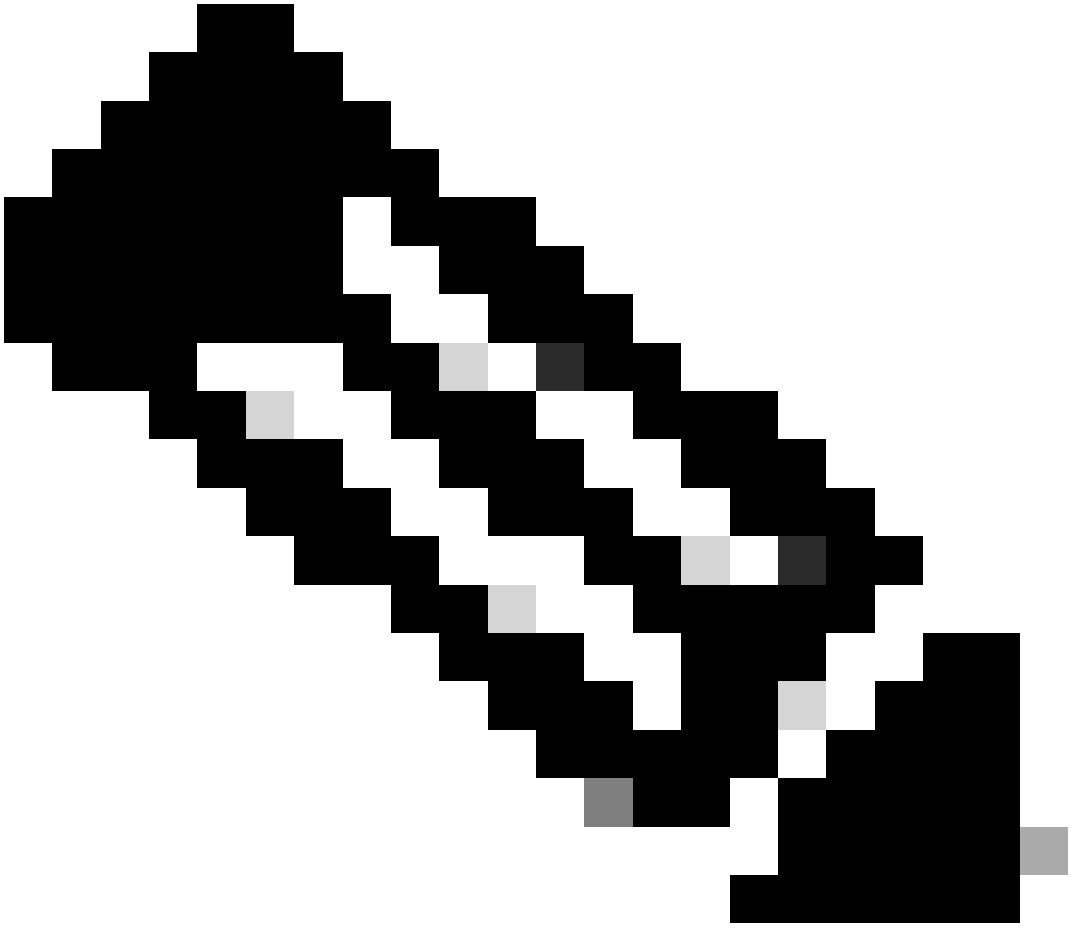
Les offres groupées CA seraient les mêmes que celles illustrées dans l'image, mais, bien sûr, il n'y aurait pas de certificat d'entité.

Dépannage

Si vous devez remplacer un certificat expiré pour tous les services, à l'exception des certificats de base de données, la méthode la plus simple consiste à télécharger de nouveaux certificats portant le MÊME nom que les anciens certificats. Dans ce cas, le service doit simplement être redémarré et vous n'avez pas besoin de le reconfigurer.

Si vous exécutez pki csr ... et que ce nom de certificat correspond à une clé actuelle, il casse immédiatement le service. Si la production est en direct et que vous créez de manière proactive une nouvelle clé et un nouveau CSR, utilisez un nouveau nom. Vous pouvez renommer le nom actif avant de télécharger le nouveau certificat sur les serveurs.

Si les certificats de base de données ont expiré, vous devez vérifier avec l'état du cluster de base de données qui est la base de données principale, et sur tous les noeuds, exécutez la commande database cluster remove. Ensuite, vous pouvez utiliser les instructions de l'étape 3. Générez le CSR du cluster de base de données et utilisez une autorité de certification intégrée pour les signer.



Remarque : Si vous devez renouveler les certificats Cisco Meeting Manager (CMM), reportez-vous à la vidéo suivante : Mise à jour du certificat SSL de gestion des réunions Cisco.

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.