Générer et ajouter les certificats requis pour l'installation du cloud privé Secure Endpoint à partir de 3.x

Table des matières

Introduction

Ce document décrit le processus de génération de certificats qui doivent être téléchargés à chaque nouvelle installation du cloud privé de la console sécurisée ou pour renouveler les services de certificats installés.

Conditions préalables

Exigences

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

- Windows Server 2008
- CentOS 7/8
- Cloud privé virtuel de console sécurisée 3.0.2 (à partir de)
- OpenSSL 1.1.1

Composants utilisés

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Windows Server 2008 (à partir de)
- Installation du cloud privé Secure Console
- Infrastructure à clé publique
- OpenSSL
- CLI Linux

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.

Informations générales

Avec l'introduction de Secure Console Private Cloud 3.X, les noms d'hôte et les paires certificat/clé sont requis pour tous les services suivants :

- Portail d'administration
- Authentification (nouveauté dans le cloud privé 3.X)
- Console sécurisée
- Serveur de disposition
- Disposition Server - Protocole étendu
- Service De Mise À Jour De La Disposition
- Centre de gestion Firepower

Ce document est présenté comme un moyen rapide de générer et de télécharger les certificats requis. Vous pouvez modifier chacun des paramètres, y compris l'algorithme de hachage, la taille de clé et d'autres paramètres, conformément à la stratégie de votre organisation, et votre mécanisme de génération de ces certificats peut ne pas correspondre à ce qui est détaillé ici.

> **Avertissement** : la procédure mentionnée ci-dessous peut varier selon la configuration de votre serveur AC. Le serveur AC de votre choix doit déjà être configuré et la configuration de ce serveur doit être terminée. La note technique suivante décrit simplement un exemple de génération de certificats et le TAC Cisco n'intervient pas dans le dépannage des problèmes liés à la génération de certificats et/ou des problèmes de serveur CA de toute sorte.

Création de certificat

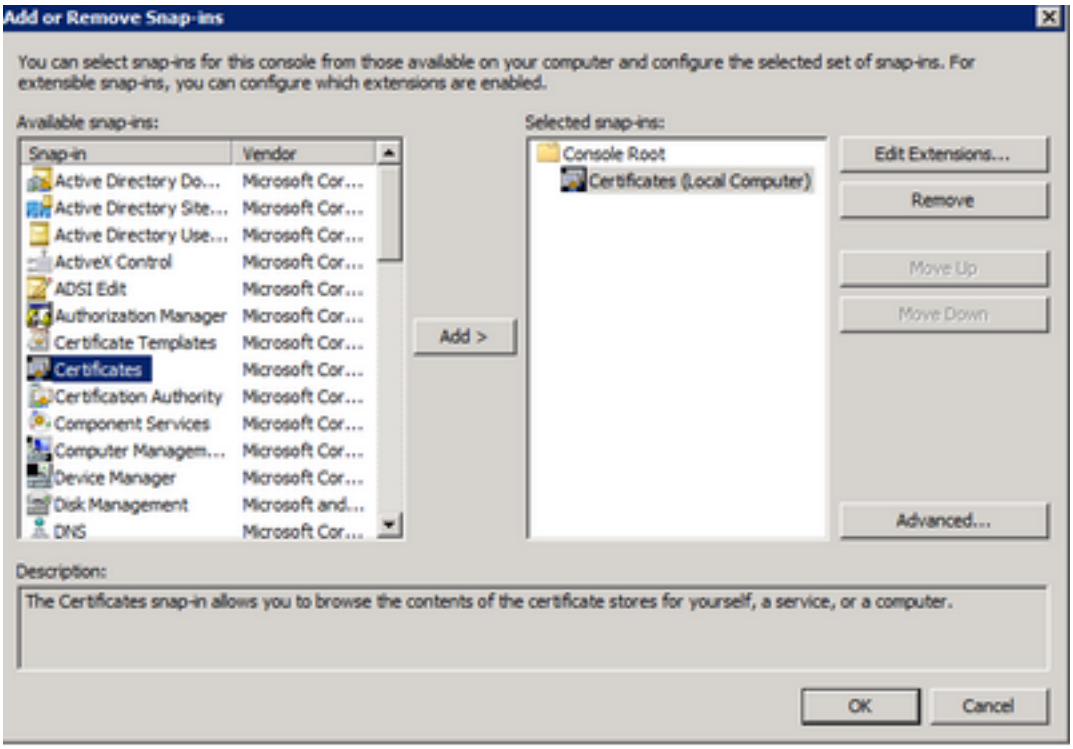
Générer des certificats sur le serveur Windows

Assurez-vous que les rôles suivants sont installés et configurés sur votre serveur Windows Server.

- Services de certificats Active Directory
- autorité de certification
- Inscription Web Autorité de certification
- Répondeur en ligne
- Service Web Inscription de certificats
- Service Web Stratégie d'inscription de certificats
- Active Directory Domain Services
- Serveurs DNS
- Serveur Web (IIS)

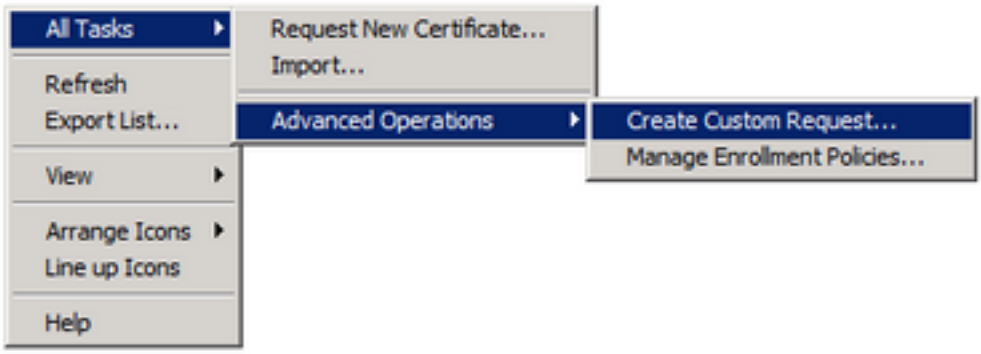
Générer une demande de signature de certificat (CSR)

Étape 1. Accédez à la console MMC et ajoutez le composant logiciel enfichable Certificats pour votre compte d'ordinateur, comme illustré dans l'image ci-contre.

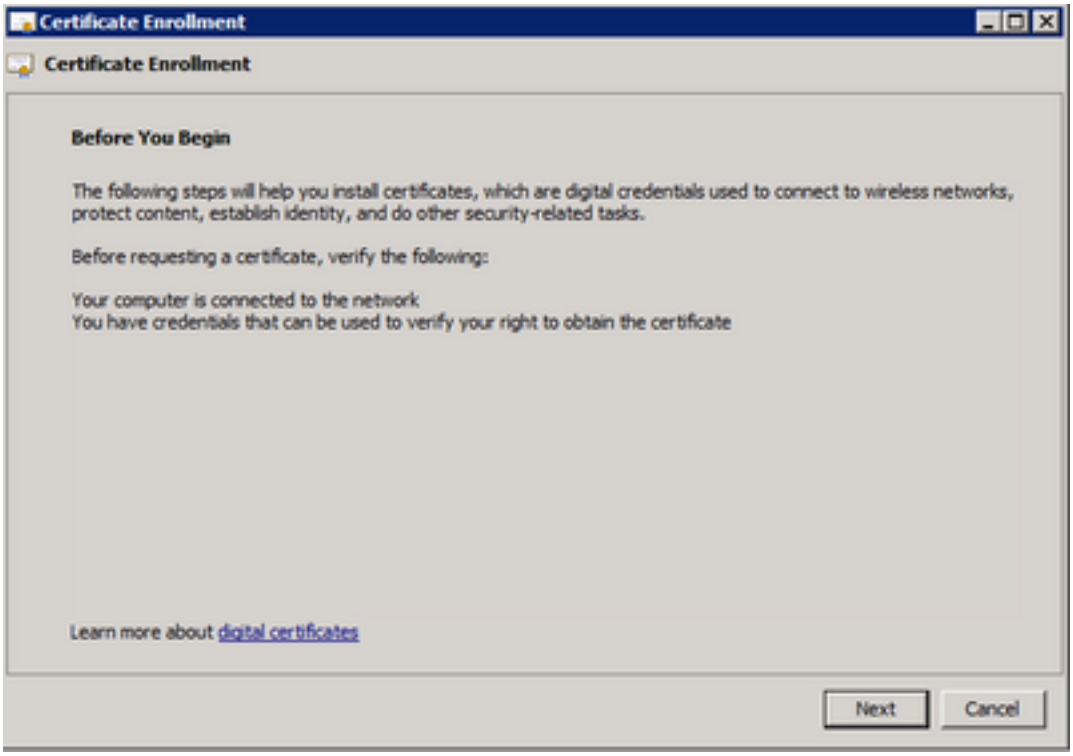


Étape 2. Développez **Certificats (Ordinateur local) > Personnel > Certificats**.

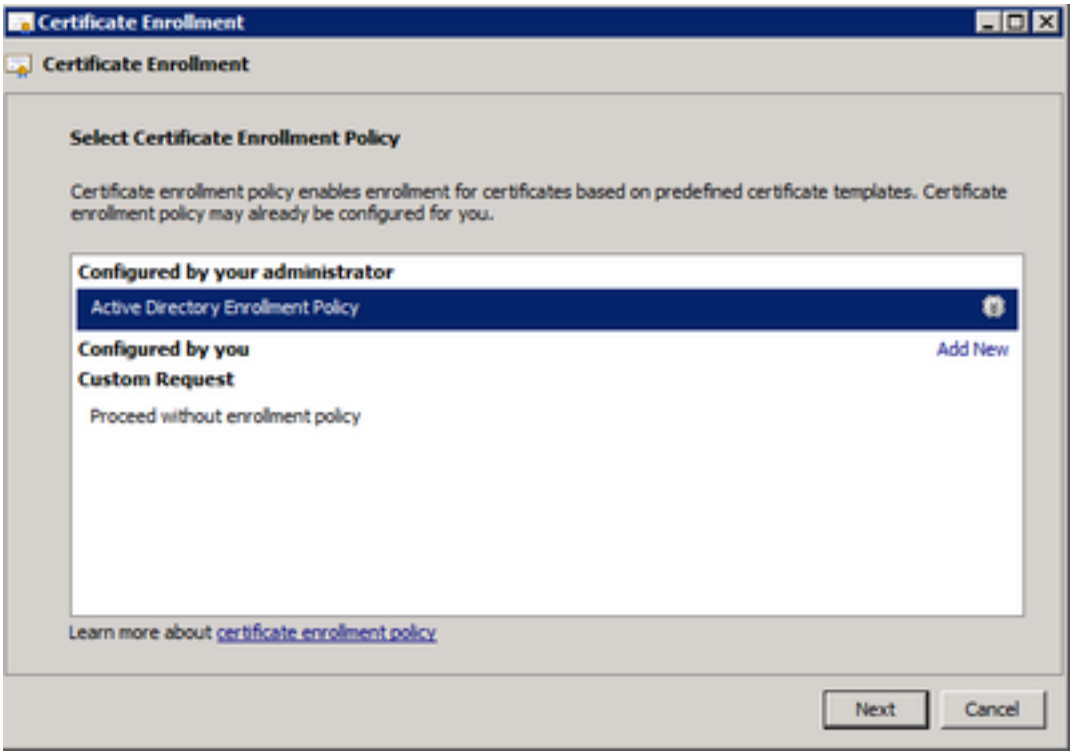
Étape 3. Cliquez avec le bouton droit sur l'espace vide et sélectionnez **Toutes les tâches > Opérations avancées > Créer une demande personnalisée.**



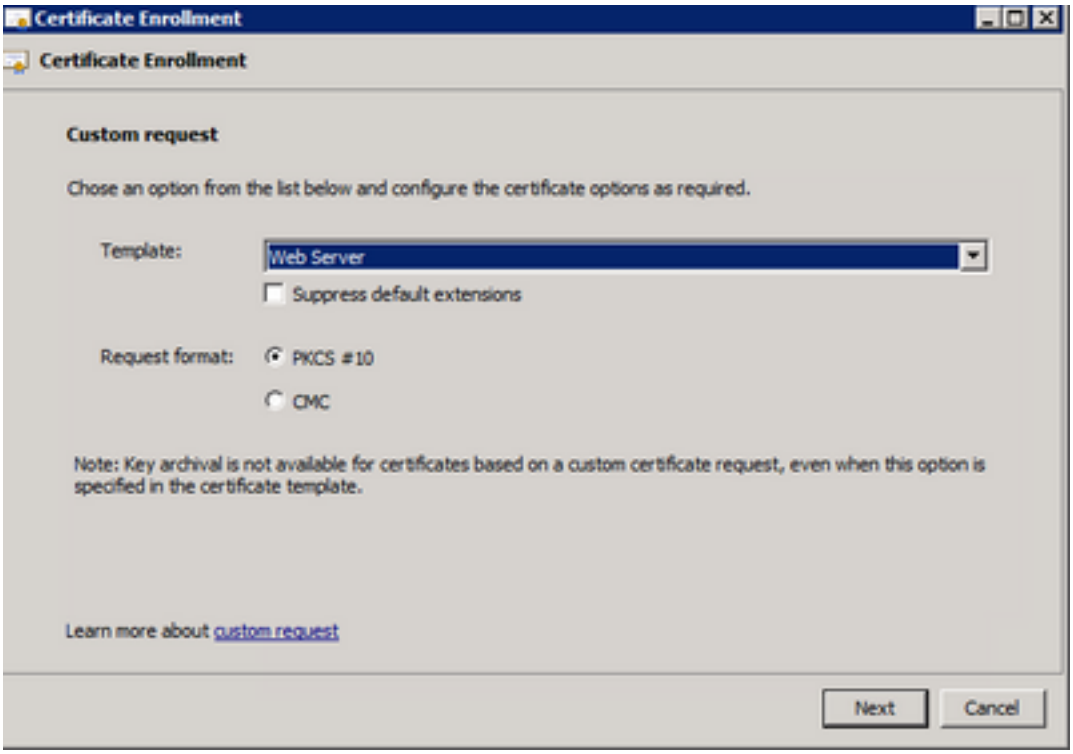
Étape 4. Sélectionnez **Suivant** dans la fenêtre Inscription.



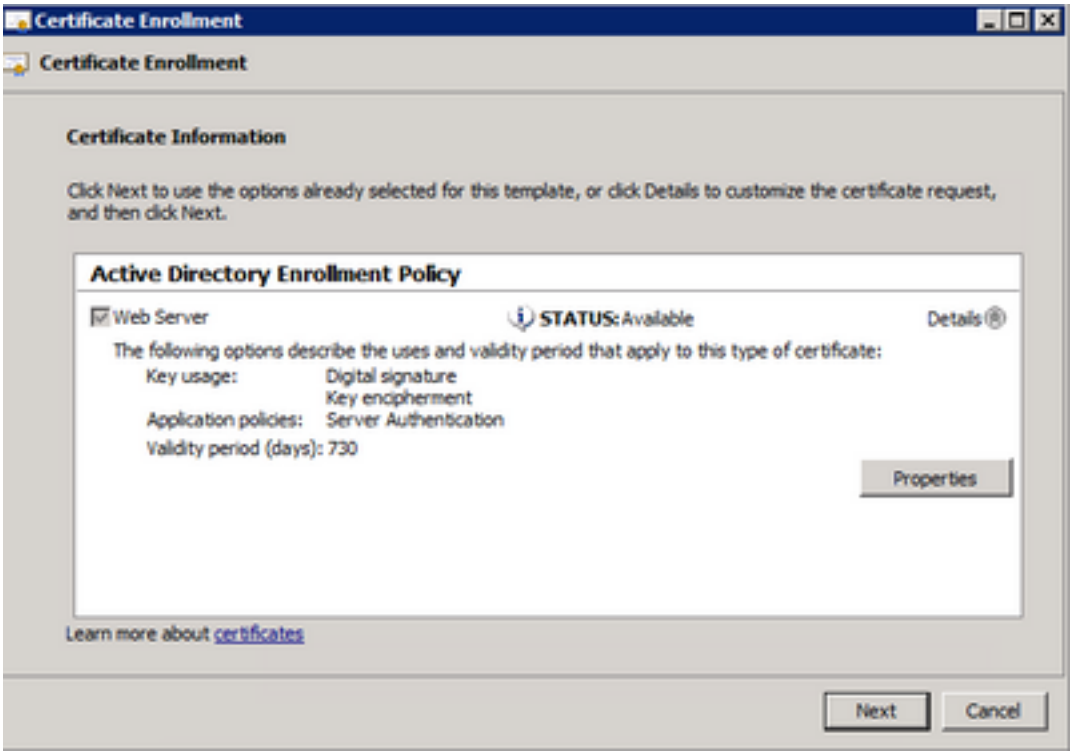
Étape 5. Sélectionnez votre stratégie d'inscription de certificat et sélectionnez **Suivant**.



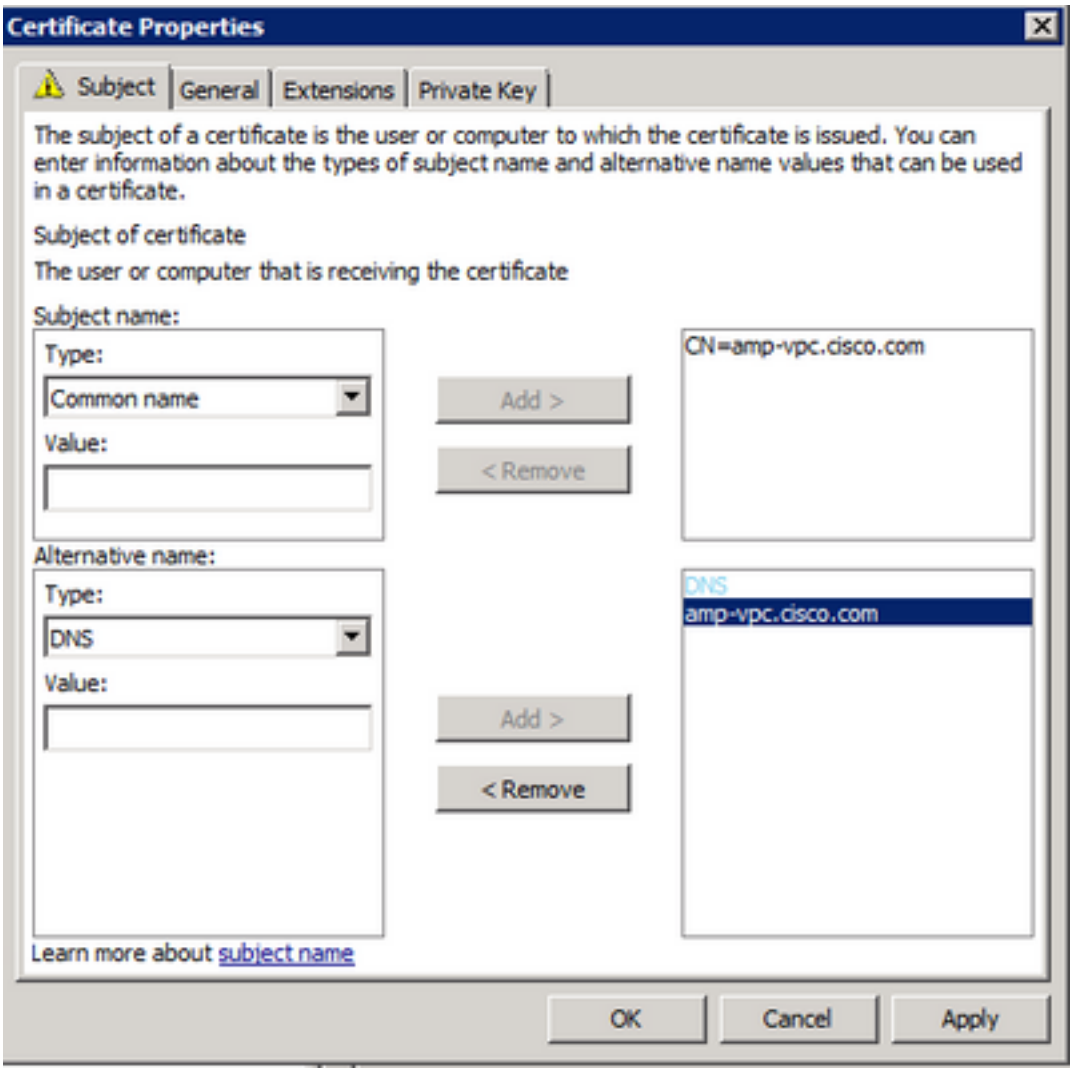
Étape 6. Choisissez le modèle comme **Serveur Web** et sélectionnez **Suivant**.



Étape 7. Si votre modèle « Serveur Web » a été configuré correctement et est disponible pour l'inscription, l'état Disponible s'affiche. Sélectionnez **Détails** pour développer Propriétés.

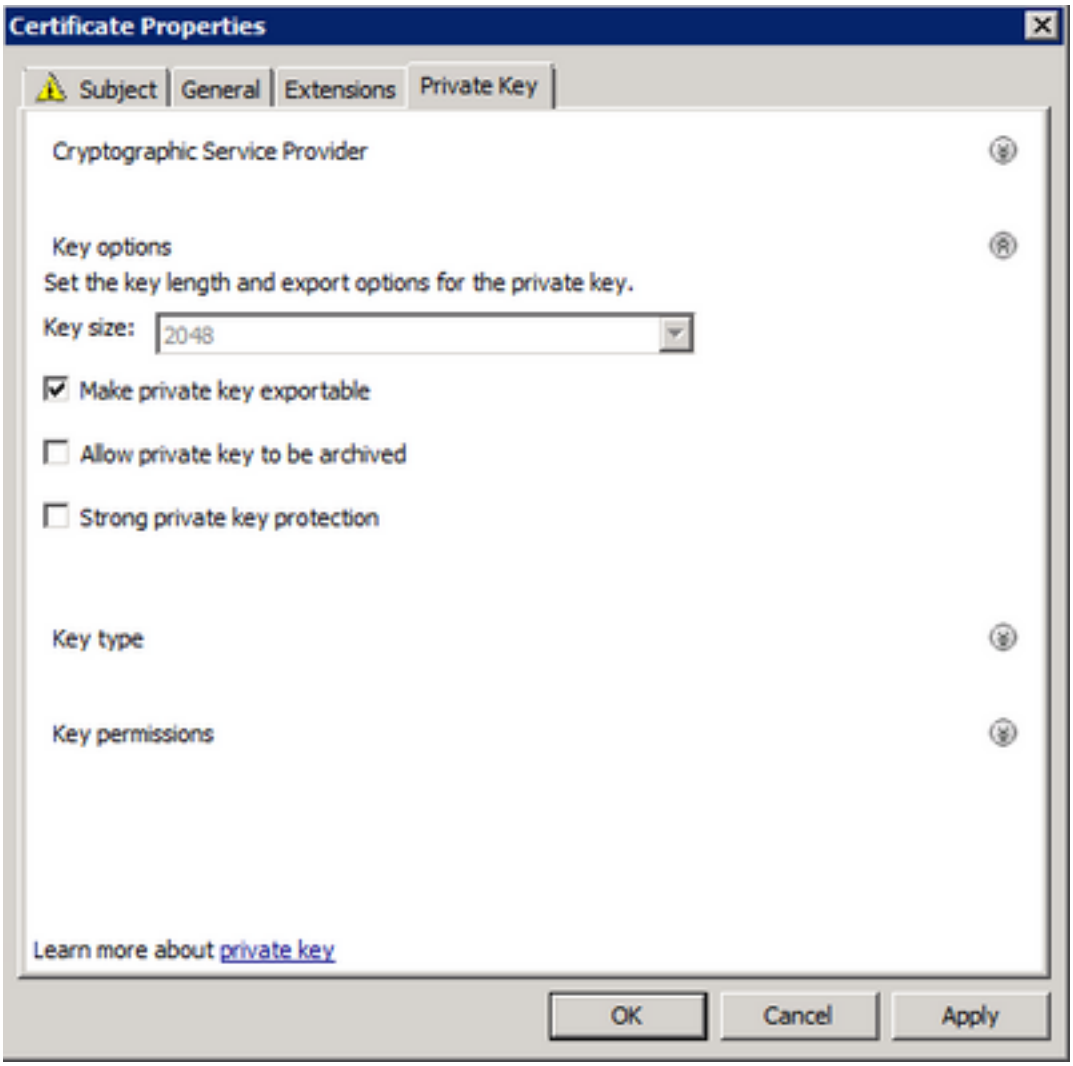


Étape 8. Ajoutez au moins les attributs CN et DNS. Le reste des attributs peut être ajouté en fonction de vos exigences de sécurité.



Étape 9. Vous pouvez éventuellement attribuer un nom convivial sous l'onglet **Général**.

Étape 10. Sélectionnez sur l'onglet **Clé privée** et assurez-vous que vous activez l'option **Rendre la clé privée exportable** sous la section **Options de clé**.

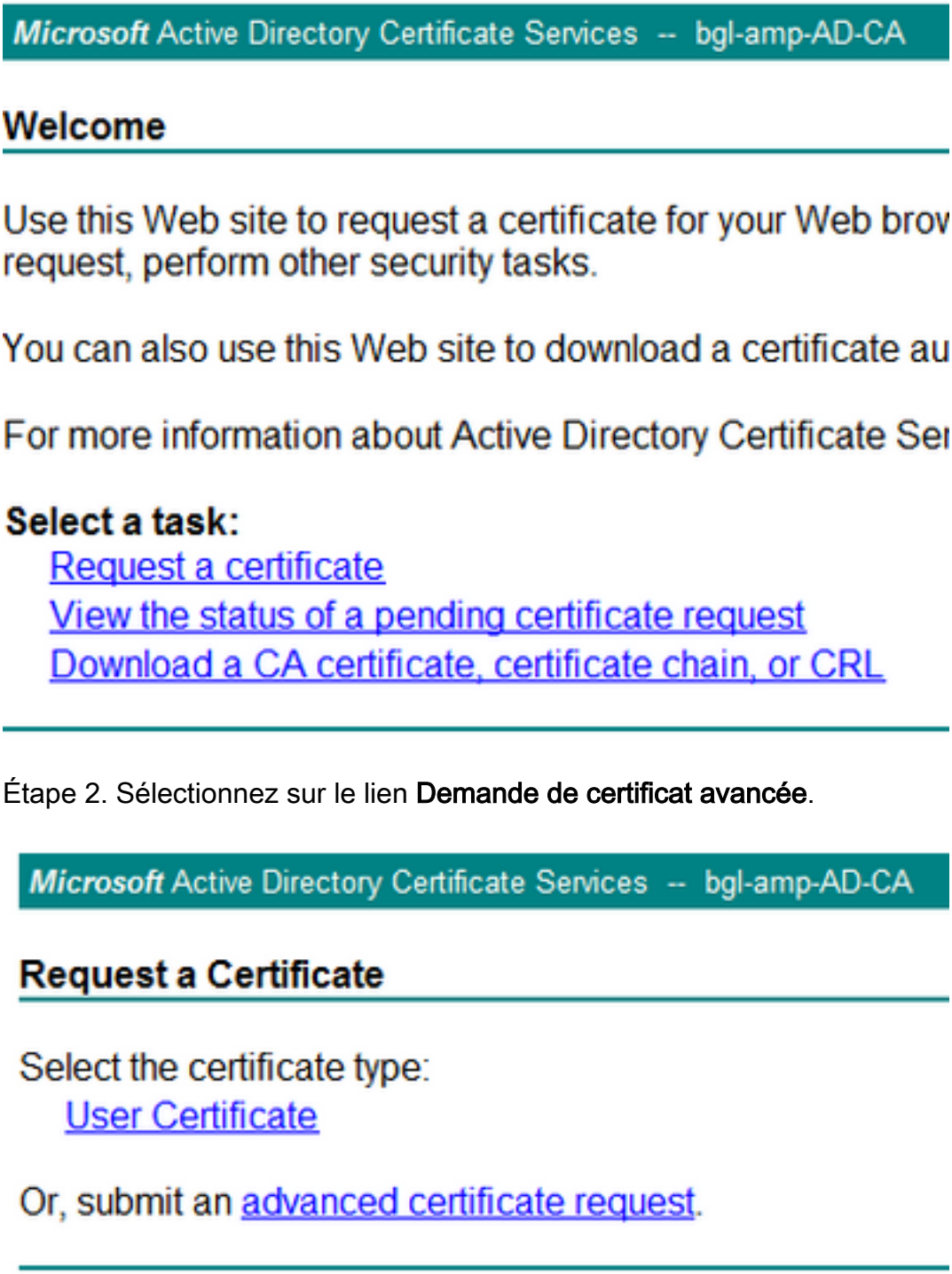


Étape 11. Enfin, sélectionnez **OK**. Vous devez alors ouvrir la boîte de dialogue Inscription de certificat dans laquelle vous pouvez sélectionner **Suivant**.

Étape 12. Accédez à un emplacement pour enregistrer le fichier .req qui est envoyé au serveur AC pour signature.

Envoi du CSR à l'autorité de certification et génération du certificat

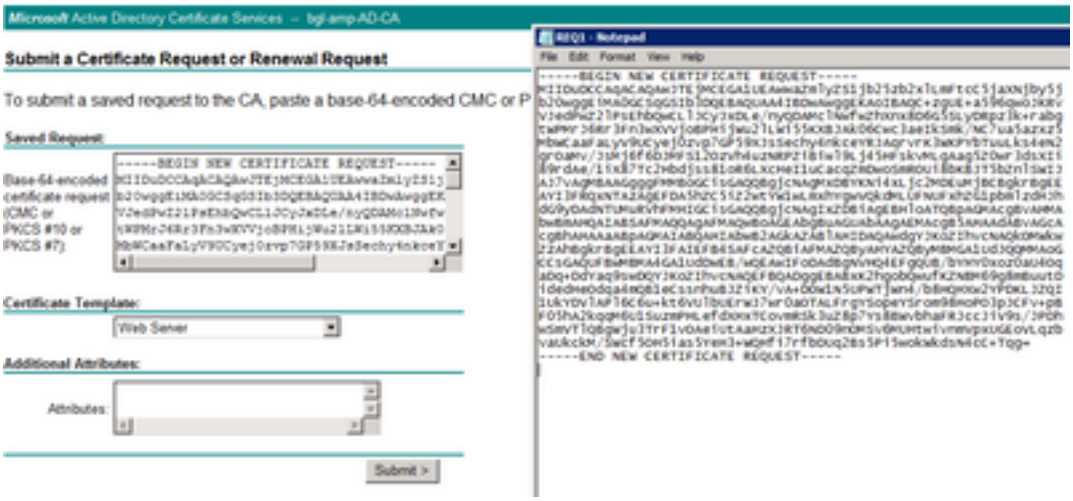
Étape 1. Accédez à votre page Web Services de certificats MS AD comme ci-dessous et sélectionnez **Demander un certificat**.



Étape 2. Sélectionnez sur le lien **Demande de certificat avancée**.

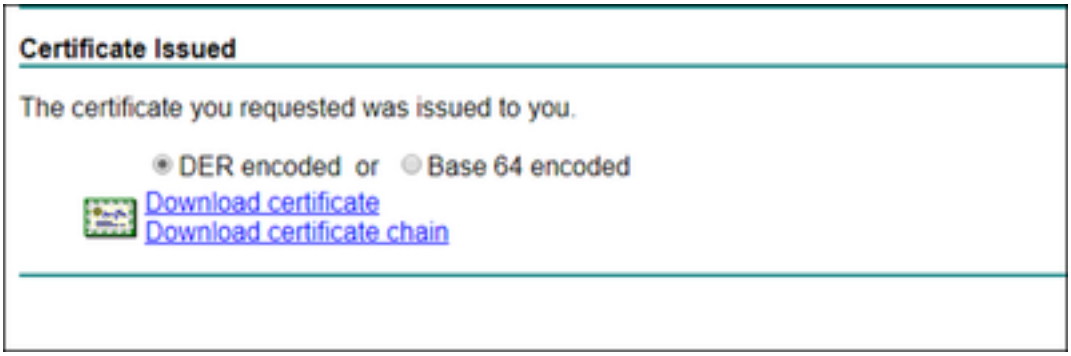
Étape 3. Sélectionnez sur **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, ou soumettez une demande de renouvellement à l'aide d'un fichier PKCS #7 encodé en base-64**.

Étape 4. Ouvrez le contenu du fichier .req (CSR) précédemment enregistré via le Bloc-notes. Copiez le contenu et collez-le ici. Assurez-vous que le modèle de certificat est sélectionné comme **serveur Web**



Étape 5. Enfin, sélectionnez **Envoyer**.

Étape 6. À ce stade, vous devez être en mesure de **Télécharger** le certificat, comme indiqué dans l'image.



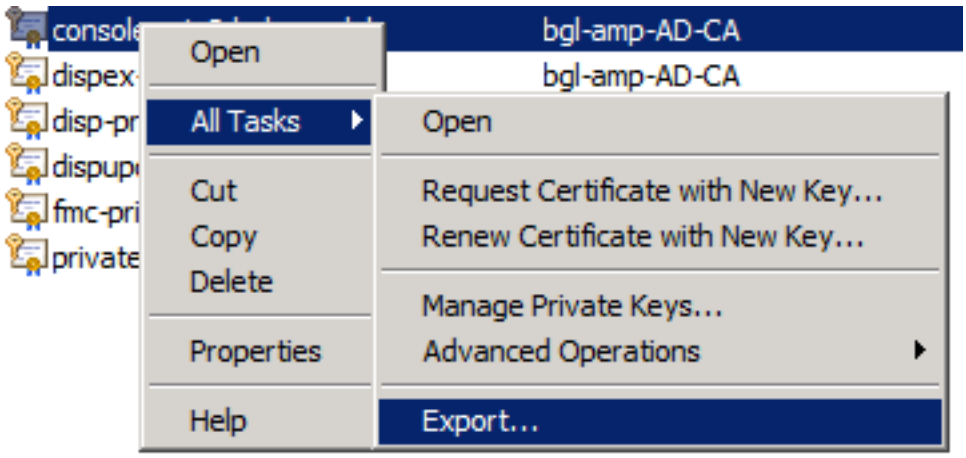
Exportation de la clé privée et conversion au format PEM

Étape 1. Installez le certificat dans votre magasin de certificats en ouvrant le fichier .cer et sélectionnez **Installer le certificat**.

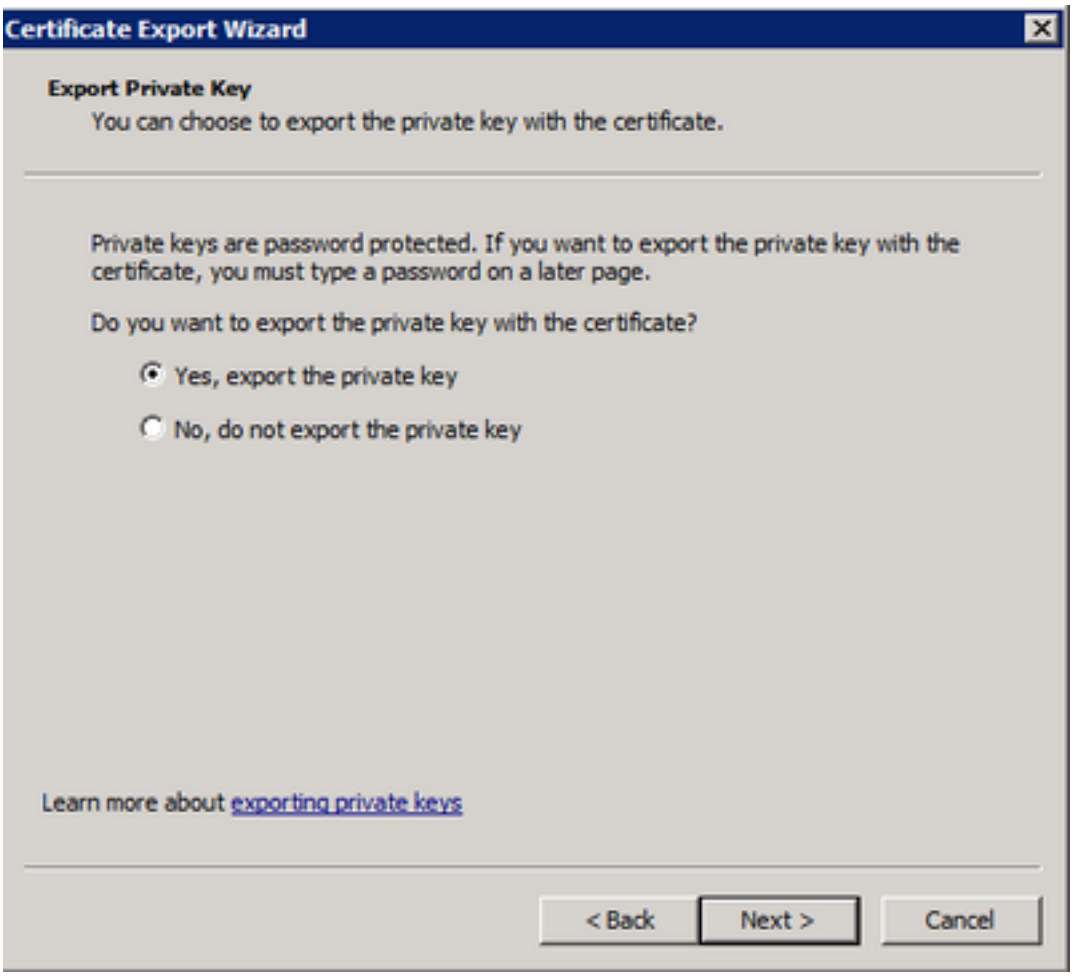
Étape 2. Accédez au composant logiciel enfichable MMC qui a été sélectionné précédemment.

Étape 3. Accédez au magasin dans lequel le certificat a été installé.

Étape 4. Cliquez avec le bouton droit sur le certificat correct, sélectionnez **Toutes les tâches > Exporter**.



Étape 5. Dans l'Assistant Exportation de certificat, confirmez l'exportation de la clé privée, comme indiqué dans l'image.



Étape 6. Entrez un mot de passe et sélectionnez **Next** pour enregistrer la clé privée sur votre disque.

Étape 7. La clé privée est ainsi enregistrée au format .PFX, mais elle doit être convertie au format .PEM pour être utilisée avec le cloud privé de point de terminaison sécurisé.

Étape 8. Installez les bibliothèques OpenSSL.

Étape 9. Ouvrez une fenêtre d'invite de commandes et accédez au répertoire dans lequel vous avez installé OpenSSL.

Étape 10. Exécutez la commande suivante pour extraire la clé privée et l'enregistrer dans un nouveau fichier : (Si votre fichier PFX ne se trouve pas dans le même chemin que celui où la bibliothèque OpenSSL est stockée, vous devez spécifier le chemin exact avec le nom du fichier)

```
openssl pkcs12 -in yourpfxfile.pfx -nocerts -out privatekey.pem -nodes
```

Étape 11. Exécutez à présent la commande suivante pour extraire également le certificat public et l'enregistrer dans un nouveau fichier :

```
openssl pkcs12 -in yourpfxfile.pfx -nokeys -out publiccert.pem -nodes
```

Générer un certificat sur le serveur Linux (vérification SSL stricte DÉSACTIVÉE)

Remarque : Strict TLS Check vérifie que le certificat répond aux exigences TLS d'Apple. Reportez-vous au Guide d'administration pour plus d'informations.

Assurez-vous que les bibliothèques OpenSSL 1.1.1 sont installées sur le serveur Linux sur lequel vous essayez de générer les certificats requis. Nous vérifions si cette procédure et la procédure ci-dessous peuvent différer de la distribution Linux que vous exécutez. Cette partie a été documentée, comme cela a été fait sur un serveur CentOS 8.4.

Générer une autorité de certification racine autosignée

Étape 1. Générez la clé privée pour le certificat d'autorité de certification racine.

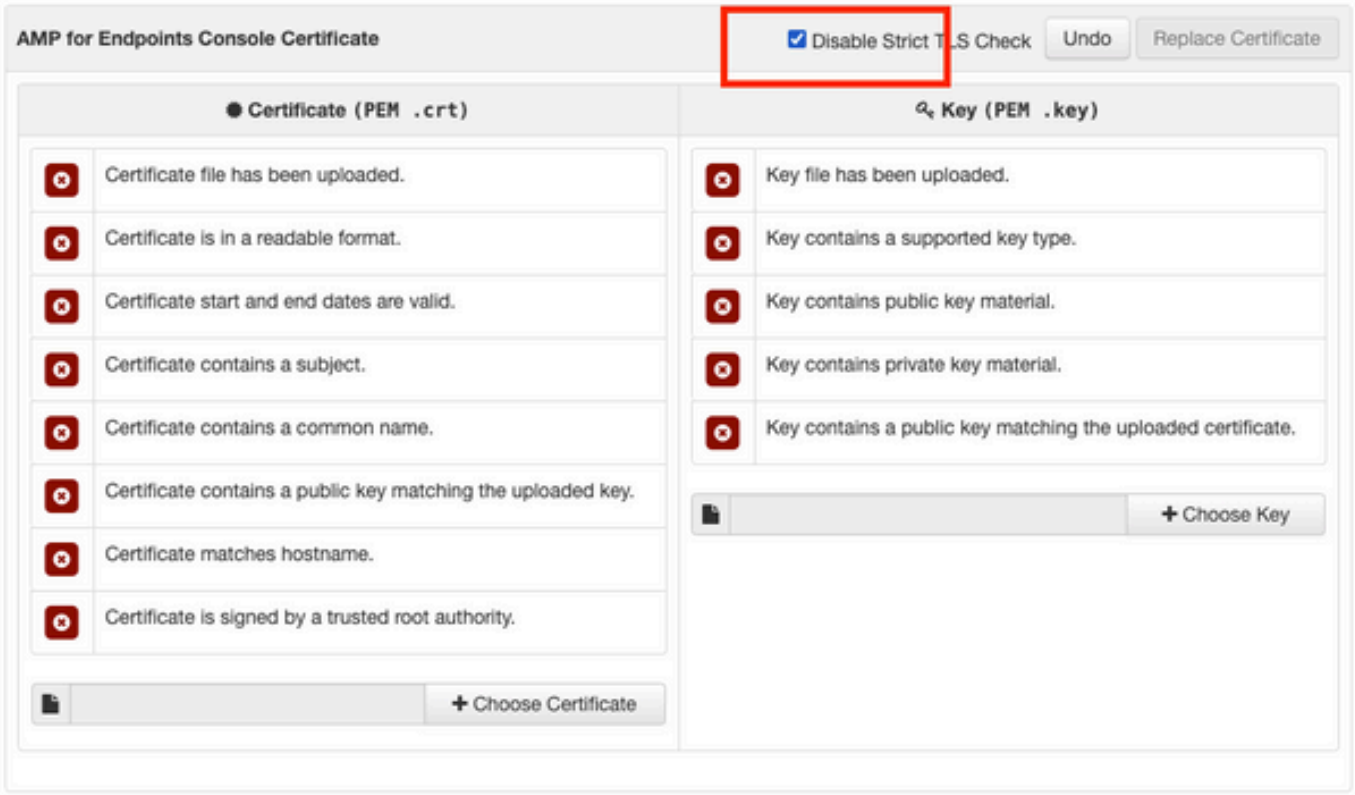
```
openssl genrsa -out
```

Étape 2. Générez le certificat CA.

```
openssl req \
-subj '/CN=
-addext "extendedKeyUsage = serverAuth, clientAuth" \
-outform pem -out
-key
-days "1000"
```

Générer un certificat pour chaque service

Créez le certificat pour le service Authentication, Console, Disposition, Disposition-Extended, Update server, Firepower Management Center (FMC) conformément à l'entrée de nom DNS. Vous devez répéter le processus de génération de certificat ci-dessous pour chaque service (authentification, console, etc.).



Générer une clé privée

```
openssl genrsa -out
```

Remplacez <YourServiceName.key> par le nouveau nom de fichier KEY à créer sous le nom Auth-Cert.key

Générer CSR

```
openssl req -new \
-subj '/CN=
-key
```

Remplacer le <YourServiceName.key> avec le fichier KEY de certificat actuel (ou nouveau) tel que Auth-Cert.key

Remplacez <YourServiceName.csr> par le nom de fichier CSR à créer, par exemple Auth-Cert.crt

Générer un certificat

```
openssl x509 -req \
-in
-CAkey
-days 397 -sha256
```

Remplacez <YourServiceName.csr> par un CSR de certificat réel (ou nouveau) tel que Auth-Cert.csr

Remplacez <YourRootCAName.pem> par le nom de fichier PEM réel (ou nouveau) RootCAName.pem

Remplacez <YourServiceName.key> par le fichier KEY de certificat actuel (ou nouveau), tel que Auth-Cert.key

Remplacez <YourServiceName.crt> par le nom de fichier à créer, par exemple Auth-Cert.crt

Générer un certificat sur le serveur Linux (vérification SSL stricte ACTIVÉE)

> **Remarque** : Strict TLS Check vérifie que le certificat répond aux exigences TLS d'Apple. Reportez-vous au Guide d'administration pour plus d'informations.

Générer une autorité de certification racine autosignée

Étape 1. Générez la clé privée pour le certificat d'autorité de certification racine.

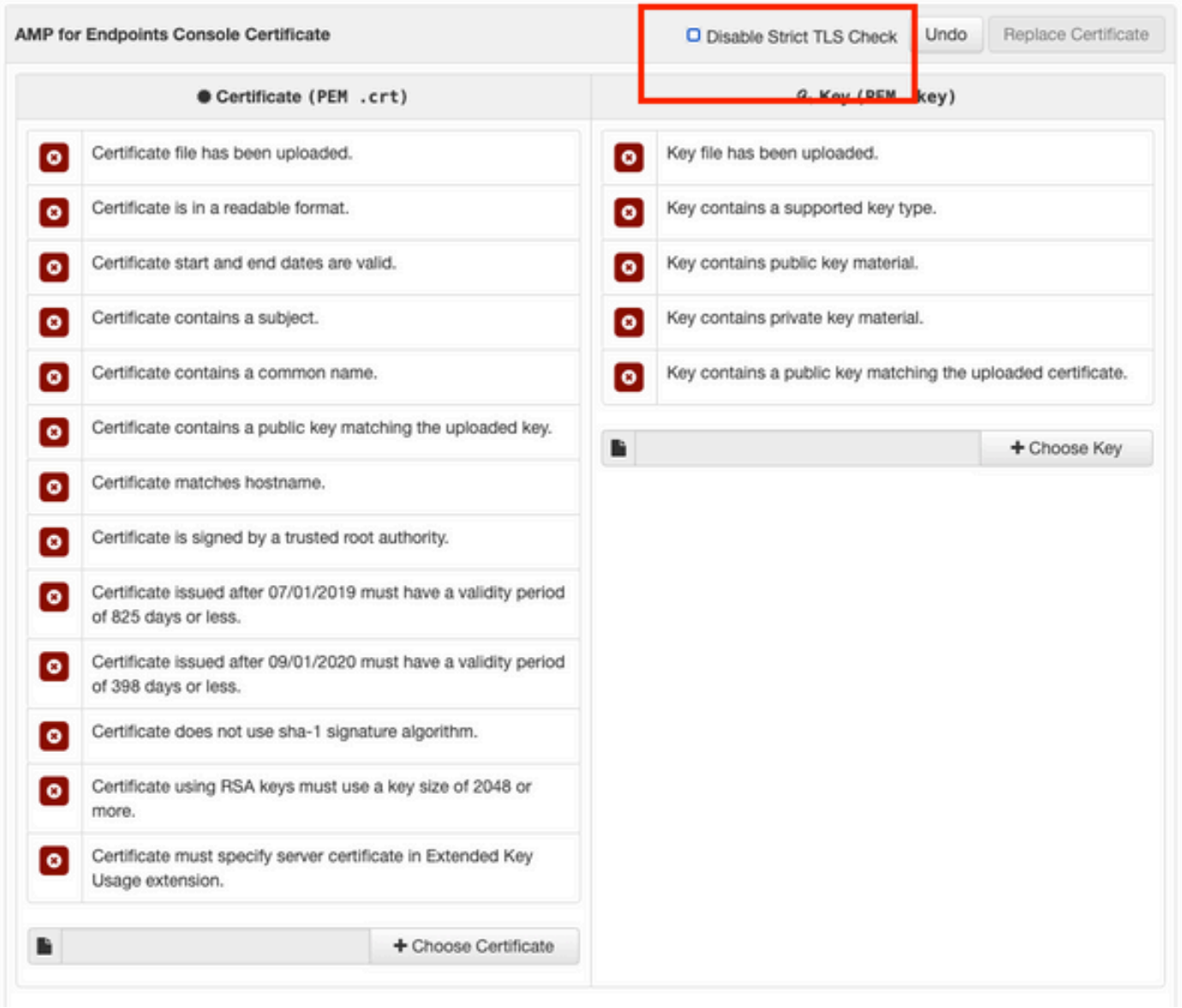
```
openssl genrsa -out
```

Étape 2. Générez le certificat CA.

```
openssl req \
-subj '/CN=
-outform pem -out
-key
-days "1000"
```

Générer un certificat pour chaque service

Créez le certificat pour le service Authentication, Console, Disposition, Disposition-Extended, Update server, Firepower Management Center (FMC) conformément à l'entrée de nom DNS. Vous devez répéter le processus de génération de certificat ci-dessous pour chaque service (authentification, console, etc.).



Créez un fichier de configuration des extensions et enregistrez-le (extensions.cnf)

```
[v3_ca]
basicConstraints = CA:FALSE
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = critical, serverAuth, clientAuth
```

Générer une clé privée

```
openssl genrsa -out
```

Remplacez <YourServiceName.key> par un nouveau nom de fichier KEY à créer en tant que Auth-Cert.key

Générer CSR

```
openssl req -new \
-key
-subj '/CN=
-out
```

Remplacer le <YourServiceName.key> avec la clé de certificat actuelle (ou nouvelle), telle que Auth-Cert.key

Remplacez <YourServiceName.csr> par le CSR de certificat actuel (ou nouveau) tel que Auth-Cert.csr

Générer un certificat

```
openssl x509 -req -in
-CA
-CAcreateserial -out
-extensions v3_ca -extfile extensions.cnf \
-days 397 -sha256
```

Remplacez <YourServiceName.csr> par le CSR de certificat actuel (ou nouveau) tel que Auth-Cert.csr

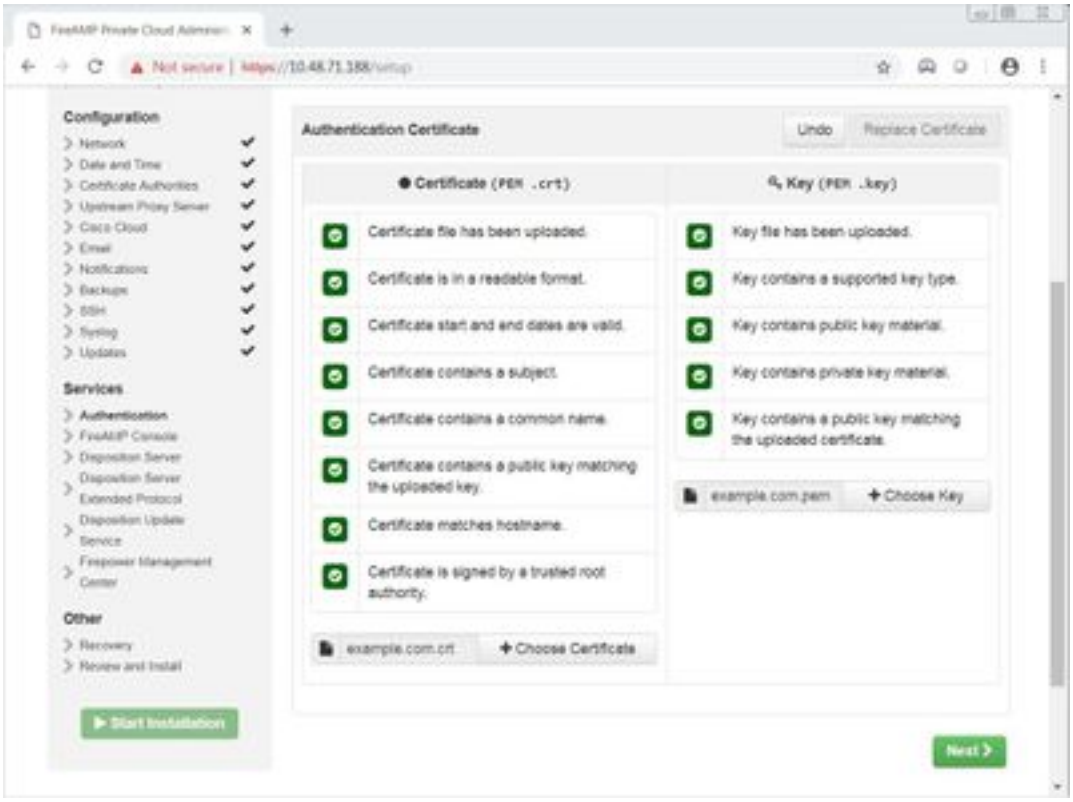
Remplacez <YourRootCAName.pem> par le nom de fichier PEM actuel (ou nouveau) RootCAName.pem

Remplacez <YourServiceName.key> par le fichier de clé de certificat actuel (ou nouveau), tel que Auth-Cert.key

Remplacez <YourServiceName.crt> par le nom de fichier à créer, par exemple Auth-Cert.crt

Ajout des certificats au cloud privé de la console sécurisée

Étape 1. Une fois que les certificats sont générés à partir de l'une des méthodes ci-dessus, téléchargez le certificat correspondant pour chacun des services. Si elles ont été générées correctement, toutes les coches sont activées comme le montre l'image ci-contre.



Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

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.