Configurer le certificat pour les serveurs gérés par Intersight

Table des matières

Introduction

Ce document décrit le processus de génération d'une demande de certificat signé (CSR) pour créer des certificats personnalisés pour les serveurs gérés par Intersight.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Intersight
- Certificats de tiers
- OpenSSL

Composants utilisés

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

- Interconnexion de fabric Cisco UCS 6454, microprogramme 4.2(1m)
- Serveur lame UCSB-B200-M5, microprogramme 4.2(1c)
- Logiciel Intersight en tant que service (SaaS)

- Ordinateur MAC avec OpenSSL 1.1.1k

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

En mode de gestion Intersight, la stratégie Gestion des certificats vous permet de spécifier les détails du certificat et de la paire de clés privées pour un certificat externe et d'associer la stratégie aux serveurs. Vous pouvez télécharger et utiliser le même certificat externe et la même paire de clés privées pour plusieurs serveurs gérés Intersight.

Configurer

Ce document utilise OpenSSL afin de générer les fichiers requis pour obtenir la chaîne de certificats et la paire de clés privées.

Étape 1.	Créez le .cnf qui contient tous les détails du certificat (il doit inclure les adresses IP pour la connexion IMC aux serveurs).
Étape 2.	Créez la clé privée et le .csr via OpenSSL.
Étape 3.	Envoyez le fichier CSR à une autorité de certification afin de signer le certificat. Si votre organisation génère ses propres certificats auto-signés, vous pouvez utiliser le fichier CSR afin de générer un certificat auto-signé.
Étape 4.	Créez la stratégie de gestion des certificats dans Intersight et collez les chaînes Certificate et Private Key-pair.

Créer le fichier de configuration (.cnf)

Utilisez un éditeur de fichier afin de créer le fichier de configuration avec une extension .cnf. Renseignez les paramètres en fonction des détails de votre organisation.

<#root>

```
[ req ]
default_bits =
```

2048

```
distinguished_name =
```

req_distinguished_name

req_extensions =

req_ext

prompt =

no

[req_distinguished_name]
countryName =

US

stateOrProvinceName =

California

localityName =

San Jose

organizationName =

Cisco Systems

commonName =

esxi01

[req_ext]
subjectAltName =

@alt_names

[alt_names]
DNS.1 =

10.31.123.60

IP.1 =

10.31.123.32

IP.2 =

10.31.123.34

IP.3 =

10.31.123.35

⚠ Attention : utilisez le ou les noms secondaires du sujet afin de spécifier des noms d'hôtes ou des adresses IP supplémentaires pour vos serveurs. Si vous ne le configurez pas ou si vous ne l'excluez pas du certificat téléchargé, les navigateurs risquent de bloquer l'accès à l'interface Cisco IMC.

Générer une clé privée (.key)

Utilisation `openssl genrsa` afin de générer une nouvelle clé.

<#root>

```
Test-Laptop$
openssl genrsa -out cert.key 2048
```

Vérifiez le fichier nommé `cert.key` est créé par le biais de `ls -la` erasecat4000_flash:.

<#root>

```
Test-Laptop$
ls -la | grep cert.key

-rw------- 1 user staff 1675 Dec 13 21:59 cert.key
```

Générer CSR

Utilisation `openssl req -new` afin de demander une `.csr` à l'aide de la clé privée `.cnf` fichiers créés précédemment.

<#root>

```
Test-Laptop$
openssl req -new -key cert.key -out cert.csr -config cert.cnf
```

Utilisation `ls -la` afin de vérifier la `cert.csr` est créé.

<#root>

```
Test-Laptop$
ls -la | grep .csr
```

```
-rw-r--r-- 1 user staff 1090 Dec 13 21:53 cert.csr
```

Remarque : si votre entreprise utilise une autorité de certification (CA), vous pouvez soumettre ce CSR afin d'obtenir le certificat signé par votre CA.

Générer le fichier de certificat

Générez le .cer avec le format de code x509.

<#root>

```
Test-Laptop$
```

openssl x509 -in cert.csr -out certificate.cer -req -signkey cert.key -days 4000

Utilisation ls -la afin de vérifier la certificate.cer est créé.

<#root>

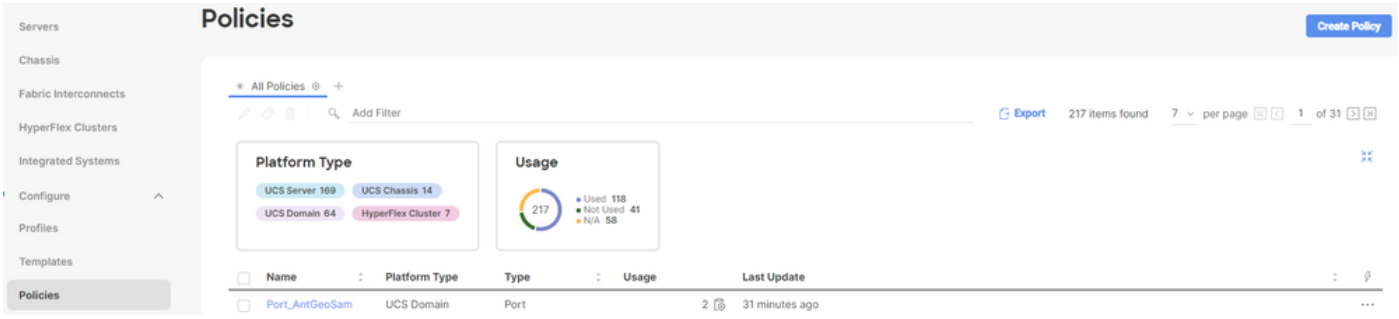
```
Test-Laptop$
```

ls -la | grep certificate.cer

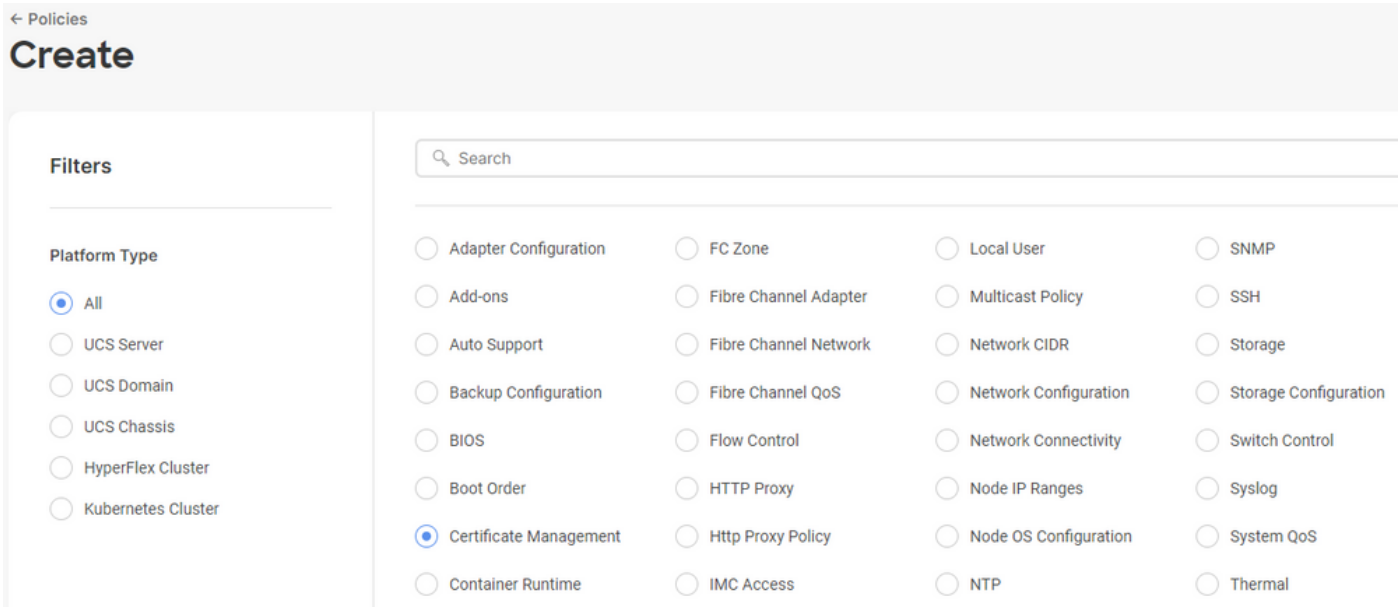
```
-rw-r--r-- 1 user staff 1090 Dec 13 21:54 certificate.cer
```

Créer la stratégie de gestion des certificats dans Intersight

Connectez-vous à votre compte Intersight, accédez à Infrastructure Service, cliquez sur le bouton Policies , puis cliquez sur le bouton Create Policy.



Filtrer par serveur UCS et choisir Certificate Management.



Utilisez **cat** Afin de copier le contenu du certificat (certificate.cert) et le fichier de clé (cert.key) et collez-les dans la stratégie de gestion des certificats dans Intersight.

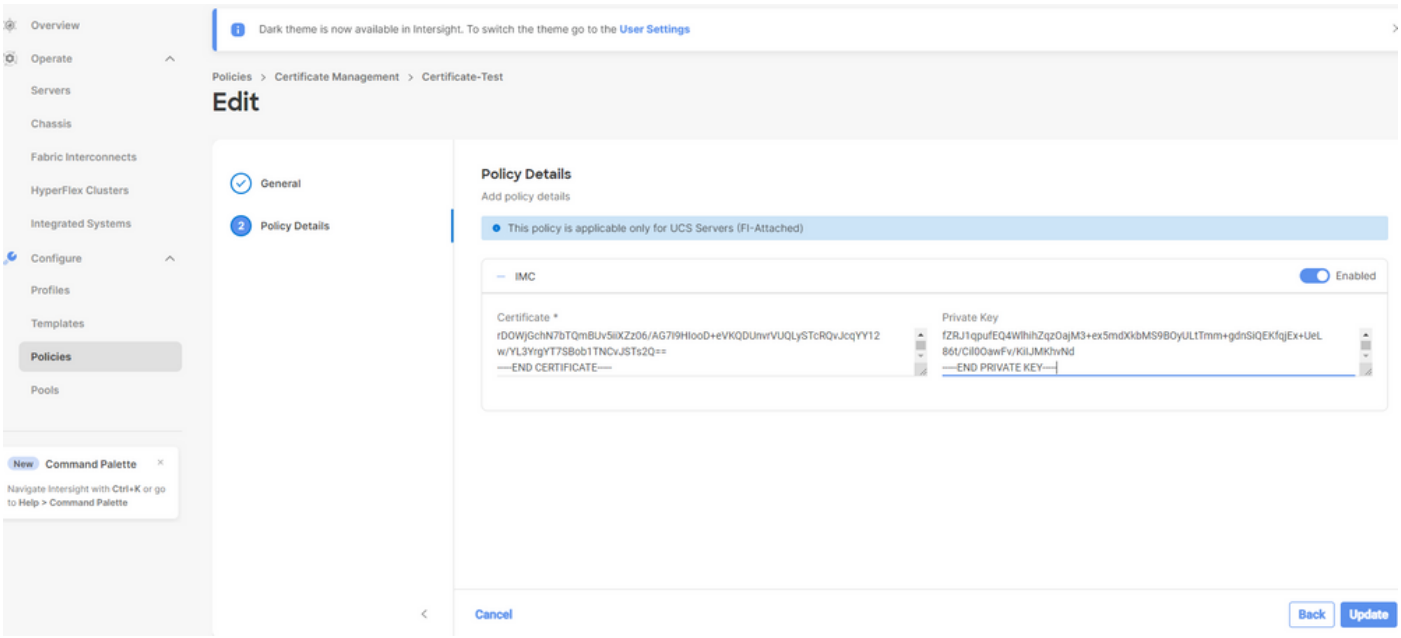
<#root>

Test-Laptop$

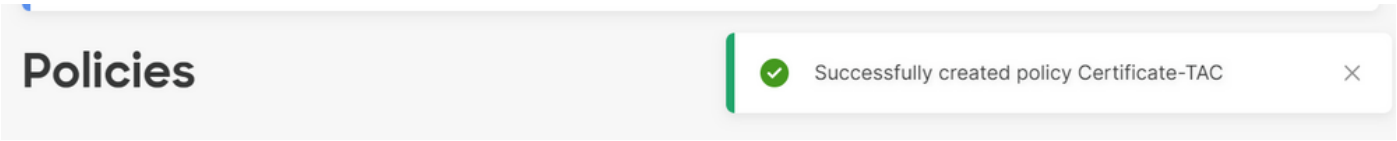
cat certificate.cert

Test-Laptop$

cat cert.key

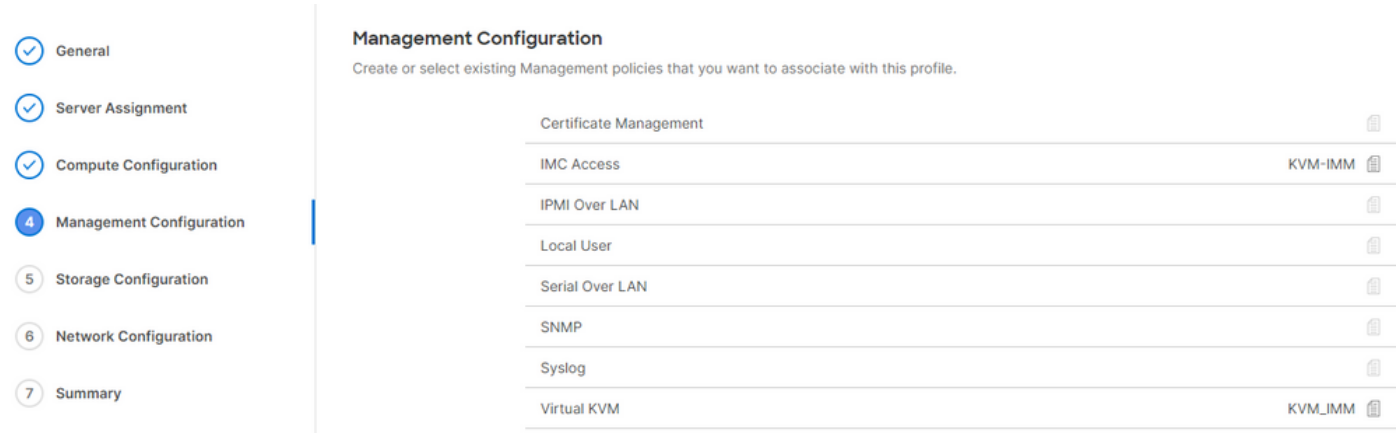


Vérifiez que la stratégie est créée sans erreur.



Ajouter la stratégie à un profil de serveur

Accédez à la page Profiles et modifiez un profil de serveur ou créez un nouveau profil et associez des stratégies supplémentaires si nécessaire. Cet exemple montre comment modifier un profil de service. Cliquer edit et continuez, associez la stratégie et déployez le profil de serveur.



Dépannage

Si vous devez vérifier les informations d'un certificat, d'un CSR ou d'une clé privée, utilisez les commandes OpenSSL mentionnées.

Afin de vérifier les détails de la RSE :

<#root>

```
Test-Laptop$
```

openssl req -text -noout -verify -in cert.csr

Afin de vérifier les détails du certificat :

<#root>

```
Test-Laptop$
```

openssl x509 -in cert.cer -text -noout

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.