Certificaat configureren voor servers die worden beheerd door Intersight

Inhoud

Inleiding

Dit document beschrijft het proces om een Certificaat Ondertekende Verzoek te produceren om aangepaste Certificaten voor servers te creëren die door Intersight worden beheerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Intersight
- Certificaten van derden
- OpenSSL

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco UCS 6454 fabric interconnect, firmware 4.2(1 m)
- UCS B-B200-M5-bladeserver, firmware 4.2(1c)
- Intersiesoftware als een service (SaaS)
- MAC Computer met OpenSSL 1.1.1k

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

In Intersight Managed Mode kunt u met het certificaatbeheerbeleid het certificaat en de privé-sleutelpaardetails voor een extern certificaat specificeren en het beleid aan servers toevoegen. U kon het zelfde externe certificaat en privé zeer belangrijk-paar uploaden en gebruiken voor de veelvoud van Intersight Beheerde Servers.

Configureren

Dit document gebruikt OpenSSL om de bestanden te genereren die nodig zijn om de certificaatketen en het privaat sleutelpaar te verkrijgen.

Stap 1.	Maak het .cnf bestand met alle details van het certificaat (het moet de IP-adressen voor de IMC verbinding met de servers bevatten).
Stap 2.	Maak de privé-sleutel en de .csr-bestanden via OpenSSL.
Stap 3.	Leg het CSR-bestand voor aan een CA om het certificaat te ondertekenen. Als uw organisatie zelf ondertekende certificaten genereert, kunt u het CSR-bestand gebruiken om een zelf-ondertekend certificaat te genereren.
Stap 4.	Maak het certificaatbeheerbeleid in Intersight en plak het certificaat en de private sleutelpaarketens.

Het configuratiebestand maken (.cnf)

Gebruik een bestandseditor om het configuratiebestand met de extensie **.cnf** te maken. Vul de instellingen in op basis van uw organisatiegegevens.

<#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

> **Waarschuwing**: gebruik de *alternatieve onderwerpnaam of -namen* om extra hostnamen of IP-adressen voor uw server(s) op te geven. Het niet configureren of uitsluiten van de adapter van het geüploade certificaat kan leiden tot het blokkeren van de toegang tot de Cisco IMC-interface door browsers.

Een privé-sleutel genereren (.key)

Gebruik **openssl genres** om een nieuwe sleutel te genereren.

<#root>

Test-Laptop$

openssl genrsa -out cert.key 2048

Controleer het genoemde bestand cert.key wordt gecreëerd via het ls -la uit.

<#root>

```
Test-Laptop$
```

```
ls -la | grep cert.key
```

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

Genereer ondertekende certificaataanvraag (CSR)

Gebruik openssl req -new om een .csr bestand met de privé-sleutel en **.cnf-**bestanden die eerder zijn gemaakt

<#root>

```
Test-Laptop$
```

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

Gebruik ls -la om de cert.csr wordt gemaakt.

<#root>

```
Test-Laptop$
```

```
ls -la | grep .csr
```

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

> **Opmerking**: als uw organisatie een certificeringsinstantie (CA) gebruikt, kunt u deze CSR indienen om het certificaat te laten ondertekenen door uw CA.

Het certificaatbestand genereren

Genereer het .cer bestand met x509-codering.

<#root>

```
Test-Laptop$
```

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

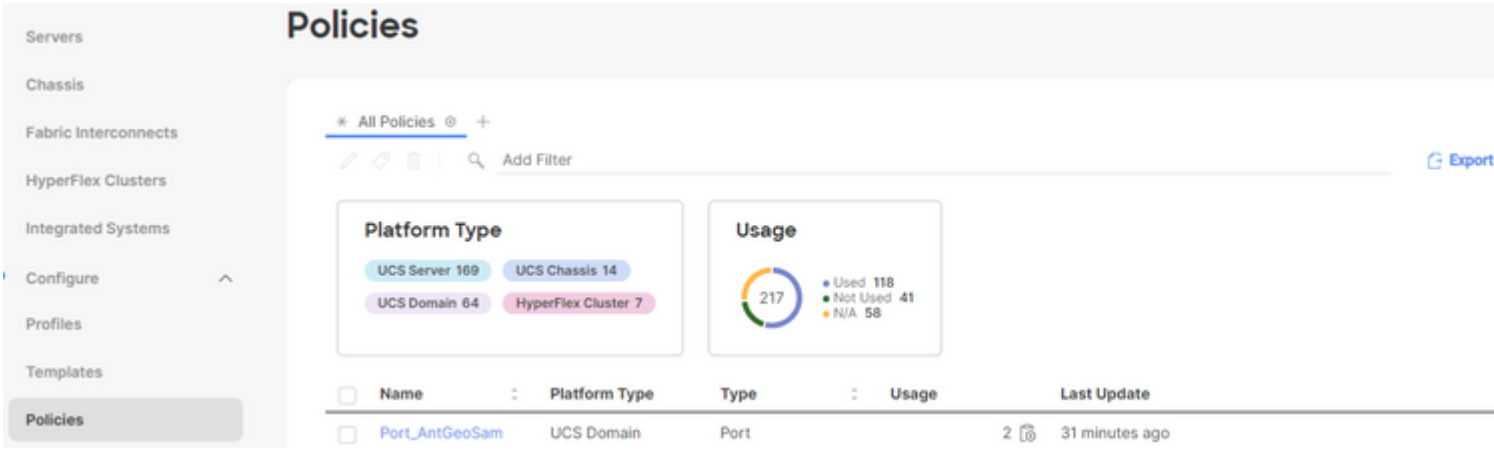
Gebruik ls -la om de certificate.cer wordt gemaakt.

<#root>

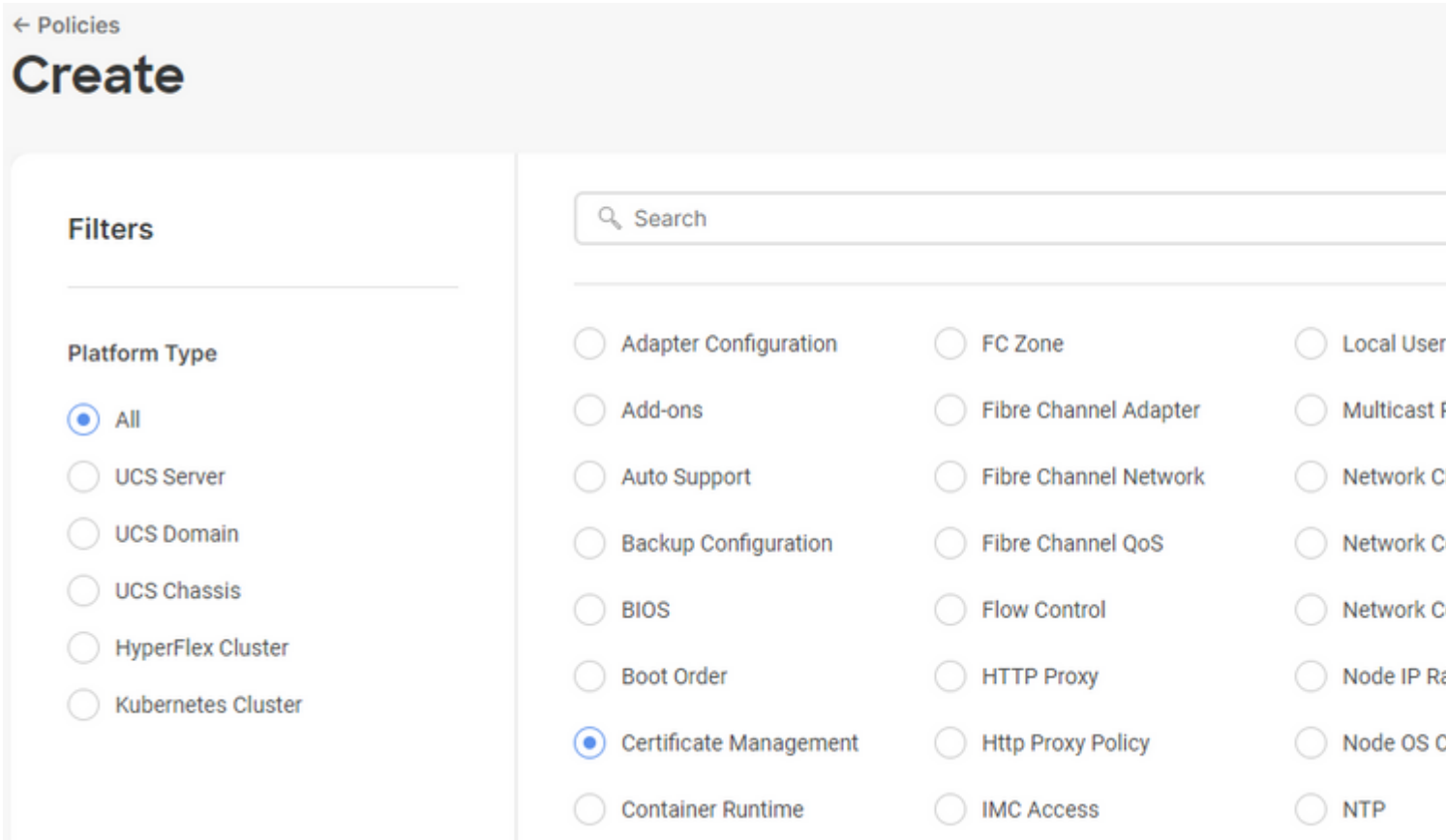
```
Test-Laptop$
ls -la | grep certificate.cer

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

Het certificaatbeheerbeleid in Intersight maken

Meld u aan bij uw Intersight-account, navigeer naar de Infrastructuurservice, klik op het tabblad Beleid en klik op Beleid maken.



Filter op UCS Server en kies Certificaatbeheer.



Gebruik **cat** opdracht om de inhoud van het certificaat te kopiëren (certificate.cert bestand) en het sleutelbestand (cert.key bestand) en plak ze op het certificaatbeheerbeleid in Intersight.

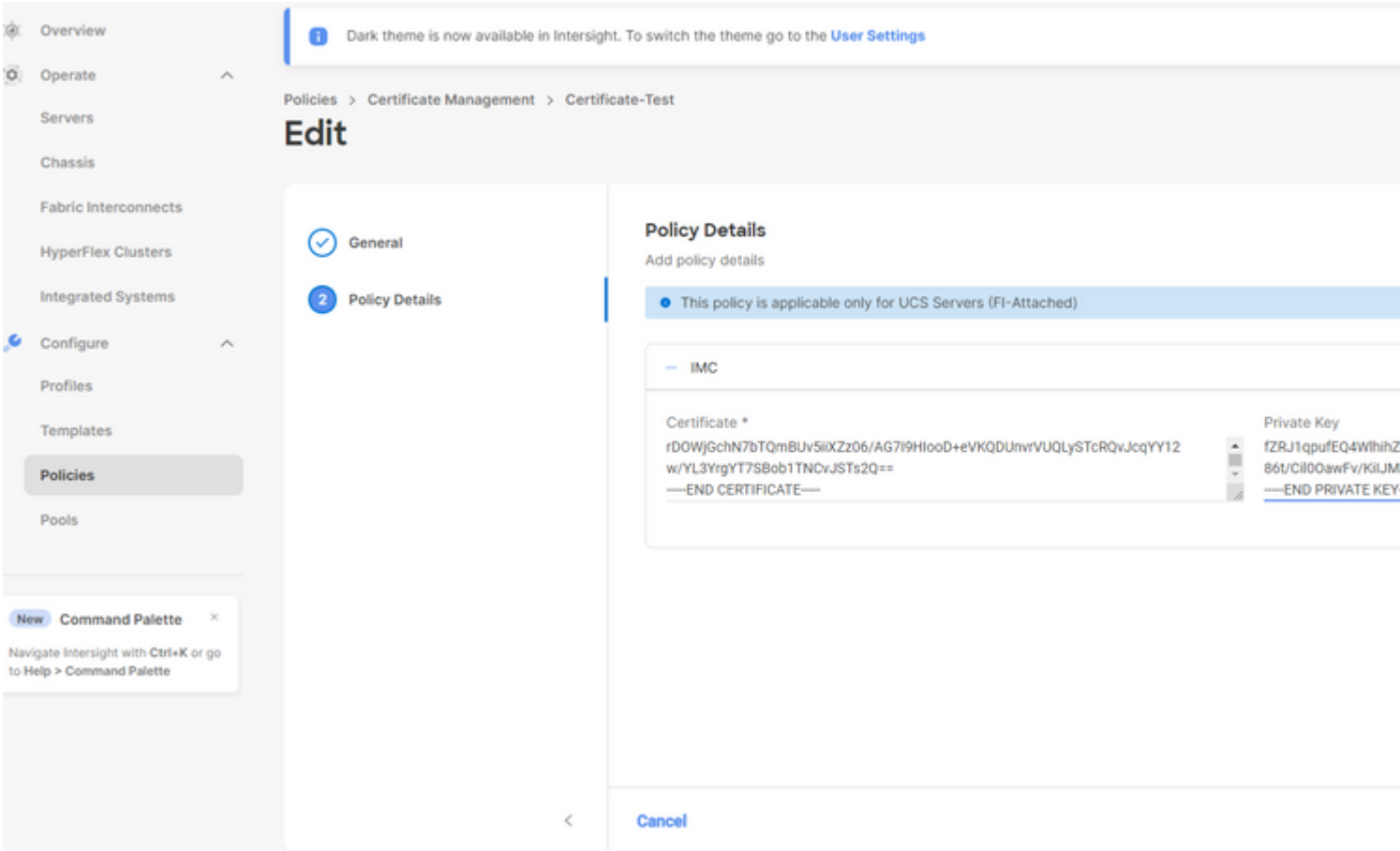
<#root>

```
Test-Laptop$
```

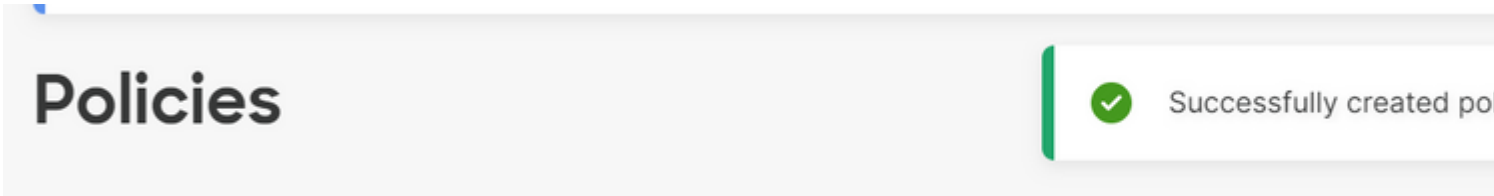
cat certificate.cert

```
Test-Laptop$
```

cat cert.key

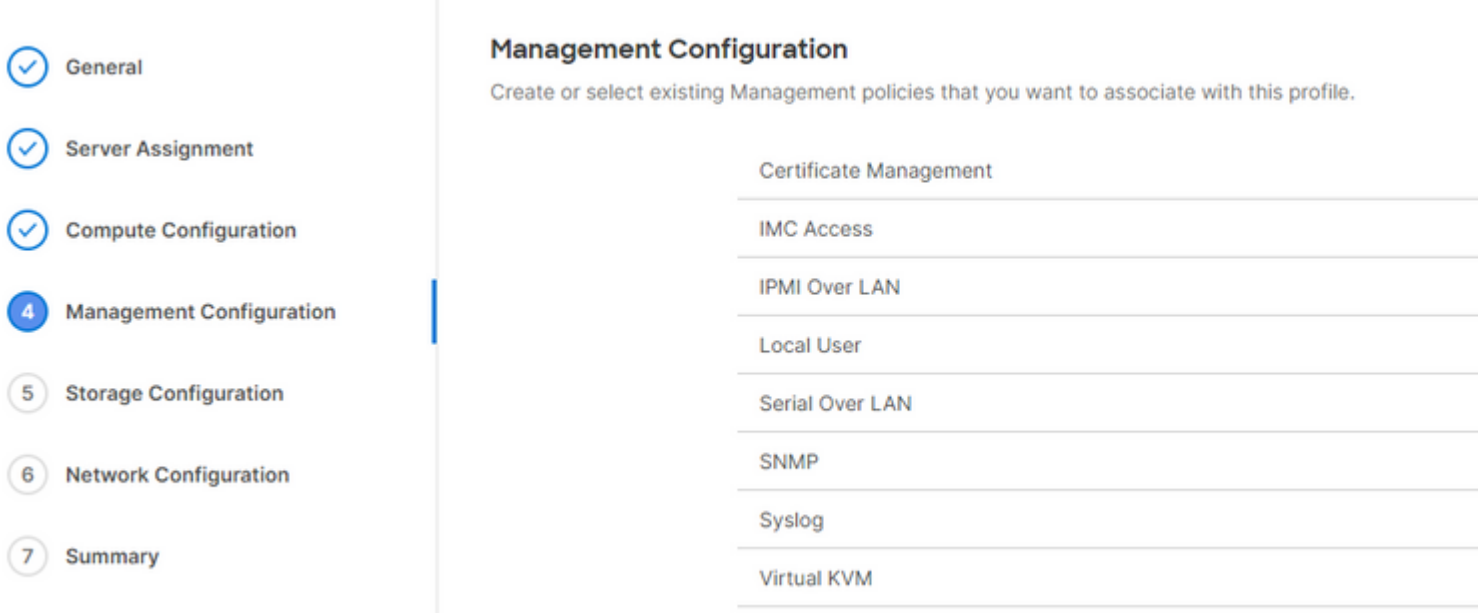


Controleer of het beleid zonder fouten is gemaakt.



Het beleid aan een serverprofiel toevoegen

Navigeer naar het tabblad Profielen en wijzig een serverprofiel of maak een nieuw profiel aan en voeg desgewenst extra beleidsregels toe. Dit voorbeeld wijzigt een serviceprofiel. Klik op bewerken en doorgaan, voeg het beleid toe en implementeer het serverprofiel.



Problemen oplossen

Als u de informatie in een certificaat, CSR of Private Key moet controleren, gebruikt u deze OpenSSL-opdrachten:

Zo controleert u de MVO-gegevens:

<#root>

```
Test-Laptop$
```

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

Zo controleert u de certificaatgegevens:

<#root>

```
Test-Laptop$
```

openssl x509 -in cert.cer -text -noout

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.