

為Intersight管理的伺服器配置證書

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[建立配置檔案\(.cnf\)](#)

[生成私鑰\(.key\)](#)

[產生CSR](#)

[生成證書檔案](#)

[在Intersight中建立證書管理策略](#)

[將策略新增到伺服器配置檔案](#)

[疑難排解](#)

簡介

本檔案介紹產生憑證簽署請求(CSR)的流程，以為Intersight管理的伺服器建立自訂憑證。

必要條件

需求

思科建議您瞭解以下主題：

- Intersight
- 第三方證書
- OpenSSL

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco UCS 6454交換矩陣互聯，韌體4.2(1m)
- UCSB-B200-M5刀鋒伺服器，韌體4.2(1c)
- Intersight軟體即服務(SaaS)
- 採用OpenSSL 1.1.1k的MAC電腦

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在Intersight託管模式下，證書管理策略允許您為外部證書指定證書和私鑰對詳細資訊並將策略附加到伺服器。您可以為多個Intersight託管伺服器上傳和使用相同的外部證書和私鑰對。

設定

本檔案使用OpenSSL來產生取得憑證鏈結和私密金鑰配對所需的檔案。

步驟 1.	建立 .cnf 包含證書的所有詳細資訊的檔案 (它必須包含用於與伺服器的IMC連線的IP地址)。
步驟 2.	建立私鑰和 .csr 通過OpenSSL上傳檔案。
步驟 3.	將CSR檔案提交到CA以簽署憑證。如果您的組織生成自己的自簽名證書，則您可以使用CSR檔案生成自簽名證書。
步驟 4.	在Intersight中建立證書管理策略並貼上證書和私鑰對鏈。

建立配置檔案(.cnf)

使用檔案編輯器建立副檔名為.cnf的配置檔案。根據您的組織詳細資訊填寫設定。

```
<#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

 注意：使用主體替代名稱為伺服器指定其他主機名或IP地址。不對其進行配置或將其從上傳的證書中排除，可能會導致瀏覽器阻止對Cisco IMC介面的訪問。

生成私鑰(.key)

使用 `openssl genrsa` 以便生成新金鑰。

<#root>

Test-Laptop\$

`openssl genrsa -out cert.key 2048`

驗證名為的檔案 `cert.key` 通過 `ls -la` 指令。

```
<#root>
Test-Laptop$
ls -la | grep cert.key

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

產生CSR


使用 `openssl req -new` 為了請求 `.csr` 檔案使用私鑰和 `.cnf` 先前建立的檔案。

```
<#root>
Test-Laptop$
openssl req -new -key cert.key -out cert.csr -config cert.cnf
```

使用 `ls -la` 以驗證 `cert.csr` 已建立。

```
<#root>
Test-Laptop$
ls -la | grep .csr

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

 註：如果您的組織使用證書頒發機構(CA)，則您可以提交此CSR，以便讓您的CA簽署證書。

生成證書檔案

生成 `.cer` x509代碼格式的檔案。

```
<#root>
Test-Laptop$
openssl x509 -in cert.csr -out certificate.cer -req -signkey cert.key -days 4000
```

使用 `ls -la` 以驗證 `certificate.cert` 已建立。

```
<#root>
```

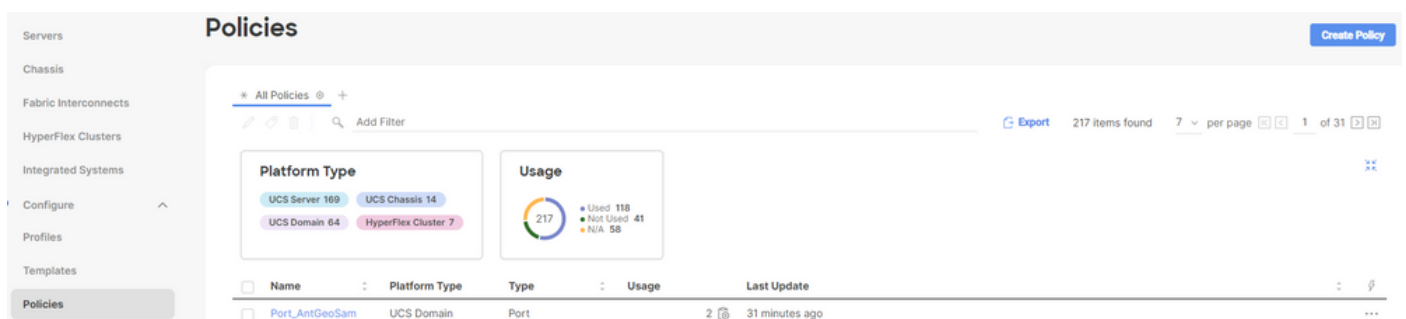
```
Test-Laptop$
```

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

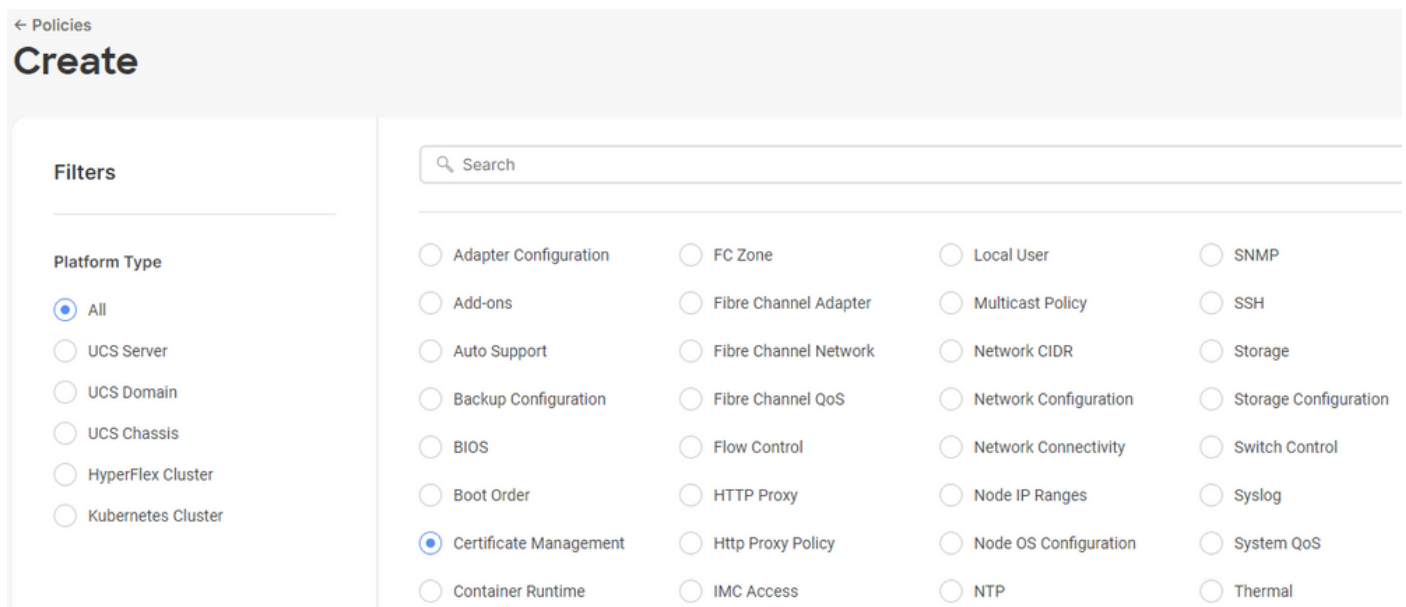
```
-rw-r--r-- 1 user staff 1090 Dec 13 21:54 certificate.cert
```

在Intersight中建立證書管理策略

登入您的Intersight帳戶，導航至 Infrastructure Service，按一下 Policies 頁籤，然後按一下 Create Policy。



按UCS伺服器過濾並選擇 Certificate Management。



使用 `cat` 命令複製憑證的內容(`certificate.cert` 檔案)和金鑰檔案(`cert.key` 檔案)並將它們貼上到Intersight中的證書管理策略中。

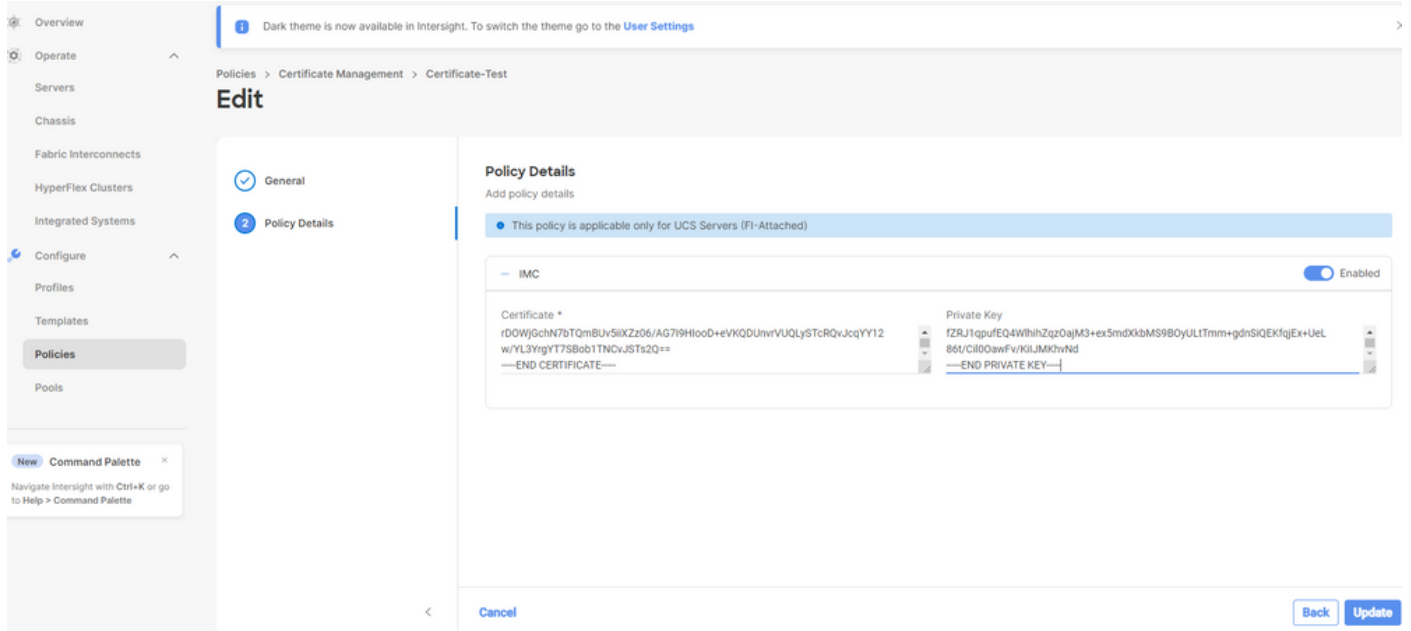
```
<#root>
```

```
Test-Laptop$
```

```
cat certificate.cert
```

```
Test-Laptop$
```

```
cat cert.key
```

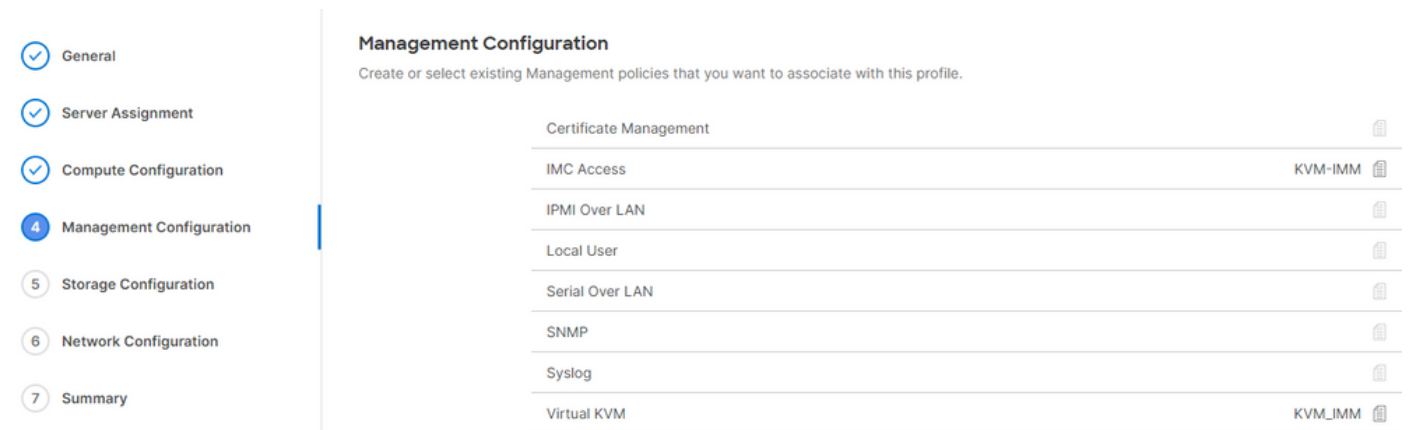


驗證是否已建立無錯誤的策略。



將策略新增到伺服器配置檔案

導航至 Profiles 頁籤並修改伺服器配置檔案，或者建立新的配置檔案並附加其他策略（如果需要）。此示例修改服務配置檔案。按一下 edit 然後繼續，附加策略，並部署伺服器配置檔案。



疑難排解

如果您需要檢查憑證、CSR或私鑰中的資訊，請如上所述使用OpenSSL命令。

若要檢查CSR詳細資訊：

```
<#root>
```

```
Test-Laptop$
```

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

若要檢查憑證詳細資訊：

```
<#root>
```

```
Test-Laptop$
```

```
openssl x509 -in cert.cer -text -noout
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。