

为Intersight管理的服务器配置证书

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[创建配置文件\(.cnf\)](#)

[生成私钥\(.key\)](#)

[生成 CSR](#)

[生成证书文件](#)

[在Intersight中创建证书管理策略](#)

[将策略添加到服务器配置文件](#)

[故障排除](#)

简介

本文档介绍为由Intersight管理的服务器创建自定义证书而生成证书签名请求(CSR)的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- Intersight
- 第三方证书
- OpenSSL

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco UCS 6454交换矩阵互联，固件4.2(1m)
- UCSB-B200-M5刀片服务器，固件4.2(1c)
- Intersight软件即服务(SaaS)
- 使用OpenSSL 1.1.1k的MAC计算机

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在Intersight管理模式下，证书管理策略允许您指定外部证书的证书和私钥对详细信息并将策略附加到服务器。您可以为多个Intersight托管服务器上传并使用相同的外部证书和私钥对。

配置

本文档使用OpenSSL生成获取证书链和私钥对所需的文件。

步骤 1:	创建 .cnf 包含证书的所有详细信息的文件（必须包含与服务器的IMC连接的IP地址）。
步骤 2	创建私钥和 .csr 文件。
第 3 步 :	将CSR文件提交到CA以签署证书。如果您的组织生成自己的自签名证书，您可以使用CSR文件生成自签名证书。
第四步 :	在Intersight中创建证书管理策略并粘贴证书和私钥对链。

创建配置文件(.cnf)

使用文件编辑器创建扩展名为.cnf的配置文件。根据您的组织详细信息填写设置。

```
<#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：使用主题备用名称为服务器指定其他主机名或IP地址。不对其进行配置或将其从上传的证书中排除可能导致浏览器阻止对Cisco IMC接口的访问。

生成私钥(.key)

使用 `openssl genrsa` 以生成新密钥。

```
<#root>
```

```
Test-Laptop$
```

```
openssl genrsa -out cert.key 2048
```

验证名为的文件 `cert.key` 通过 `ls -la` 命令。

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

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

生成 CSR


使用 `openssl req -new` 为了请求 `.csr` 文件使用私钥和 `.cnf` 之前创建的文件。

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

使用 `ls -la` 为了验证 `cert.csr` 已创建。

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

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

 注意：如果您的组织使用证书颁发机构(CA)，您可以提交此CSR以获得CA签名的证书。

生成证书文件

生成 `.cer` x509代码格式的文件。

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

使用 `ls -la` 为了验证 `certificate.cert` 已创建。

```
<#root>
```

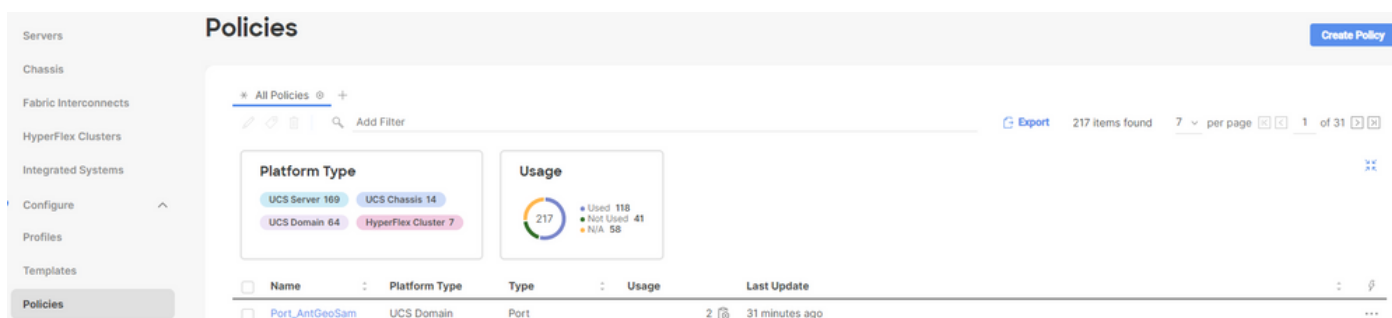
```
Test-Laptop$
```

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

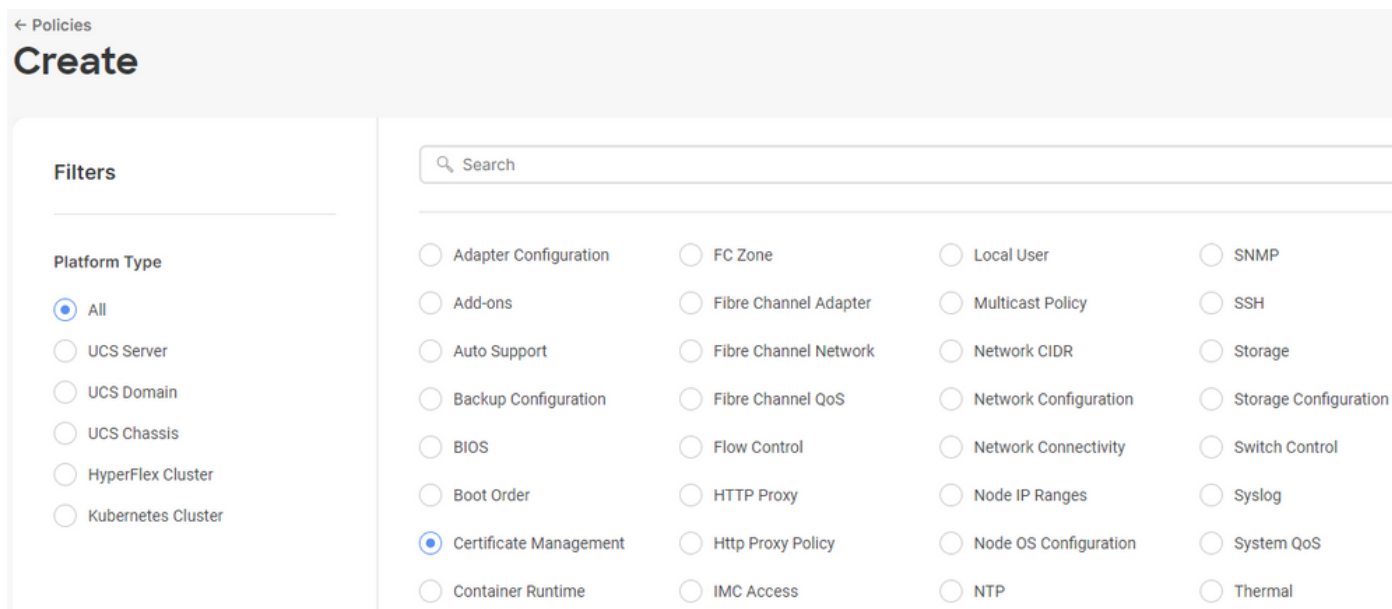
```
-rw-r--r-- 1 user staff 1090 Dec 13 21:54 certificate.cert
```

在Intersight中创建证书管理策略

登录您的Intersight帐户，导航至 Infrastructure Service, 单击 Policies 选项卡，然后单击 Create Policy.



按UCS服务器过滤并选择 Certificate Management.



请使用 `cat` 命令要复制证书的内容(`certificate.cert` 文件)和密钥文件(`cert.key` 文件)，并将它们粘贴到 Intersight中的证书管理策略中。

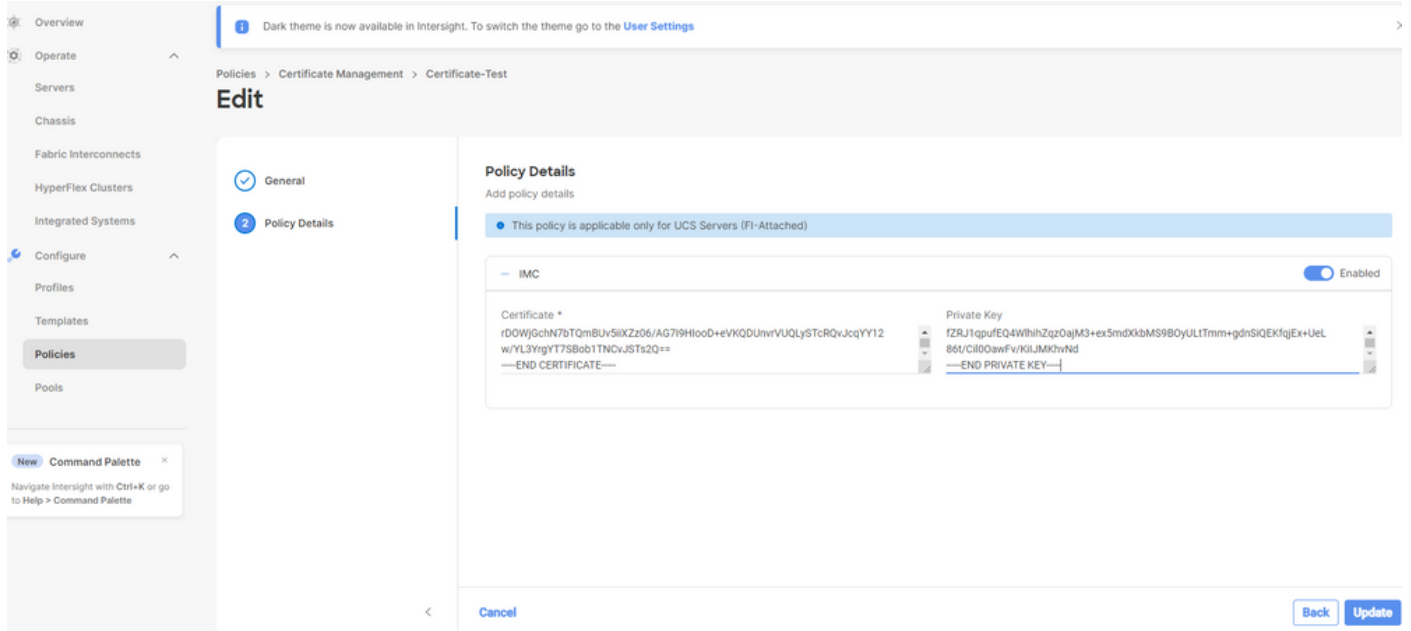
```
<#root>
```

```
Test-Laptop$
```

```
cat certificate.cert
```

```
Test-Laptop$
```

```
cat cert.key
```

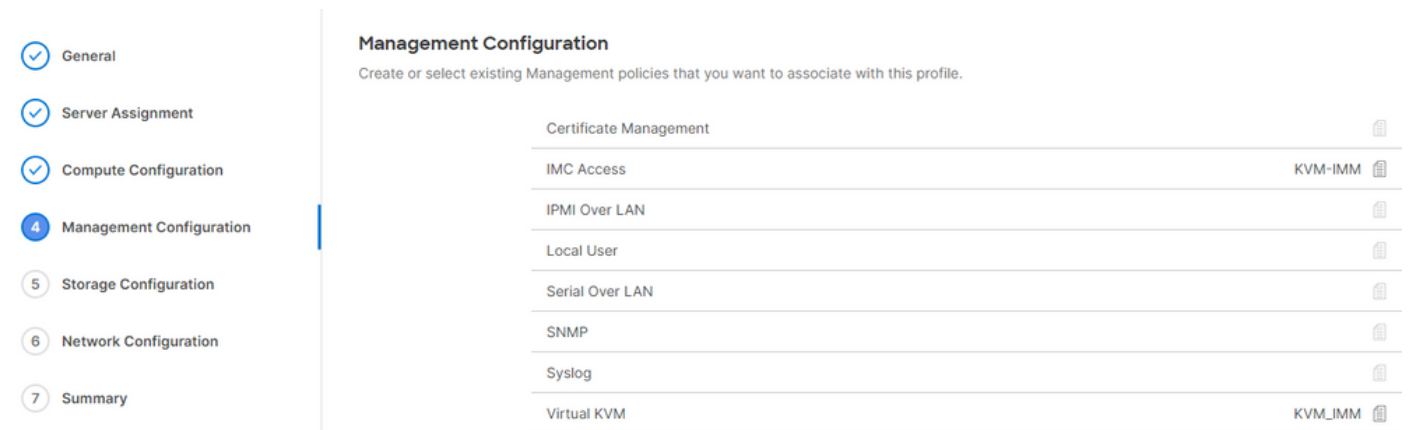


验证是否创建策略且没有错误。



将策略添加到服务器配置文件

导航至 Profiles 选项卡并修改服务器配置文件，或创建新配置文件并附加其他策略（如果需要）。此示例修改服务配置文件。点击 edit 然后继续，附加策略，并部署服务器配置文件。



故障排除

如果需要检查证书、CSR或私钥中的信息，请使用前面提到的OpenSSL命令。

要检查CSR详细信息，请执行以下操作：

```
<#root>
```

```
Test-Laptop$
```

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

要检查证书详细信息，请执行以下操作：

```
<#root>
```

```
Test-Laptop$
```

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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。