Configurar certificado para servidores administrados por Intersight

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Configurar](#)
[Crear el archivo de configuración (.cnf)](#)
[Generar una clave privada (.key)](#)
[Generar solicitud de certificado firmado (CSR)](#)
[Generar el archivo de certificado](#)
[Crear la directiva de administración de certificados en Intersight](#)
[Agregar la directiva a un perfil de servidor](#)
[Troubleshoot](#)

Introducción

Este documento describe el proceso para generar una Solicitud Firmada de Certificado para crear Certificados personalizados para servidores administrados por Intersight.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Intersight
- Certificados de terceros
- OpenSSL

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Fabric Interconnect Cisco UCS 6454, firmware 4.2(1 m)
- Servidor blade UCSB-B200-M5, firmware 4.2(1c)
- Software como servicio (SaaS) de Intersight
- Ordenador MAC con OpenSSL 1.1.1k

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En el modo administrado de intersección, la directiva de administración de certificados permite especificar los detalles del certificado y del par de claves privadas para un certificado externo y adjuntar la directiva a los servidores. Puede cargar y utilizar el mismo certificado externo y par de claves privadas para varios servidores administrados de Intersight.

Configurar

Este documento utiliza OpenSSL para generar los archivos necesarios para obtener la cadena de certificados y el par de claves privadas.

Paso 1.	Cree el archivo .cnf que contiene todos los detalles del certificado (debe incluir las direcciones IP para la conexión IMC a los servidores).
Paso 2.	Cree la clave privada y los archivos .csr mediante OpenSSL.
Paso 3.	Envíe el archivo CSR a una CA para firmar el certificado. Si su organización genera sus propios certificados autofirmados, puede utilizar el archivo CSR para generar un certificado autofirmado.
Paso 4.	Cree la directiva de administración de certificados en Intersight y pegue las cadenas de certificado y par de claves privadas.

Crear el archivo de configuración (.cnf)

Utilice un editor de archivos para crear el archivo de configuración con la extensión **.cnf**. Rellene los parámetros en función de los detalles de su organización.

<#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
```

> **Precaución**: utilice los *nombres alternativos del sujeto* para especificar nombres de host o direcciones IP adicionales para sus servidores. Si no se configura o se excluye del certificado cargado, los navegadores pueden bloquear el acceso a la interfaz de Cisco IMC.

Generar una clave privada (.key)

Utilice **openssl genrsa** para generar una nueva clave.

```
<#root>
Test-Laptop$
openssl genrsa -out cert.key 2048
```

Verifique el archivo llamado cert.key se crea a través del ls -la comando.

<#root>

```
Test-Laptop$
```

ls -la | grep cert.key

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

Generar solicitud de certificado firmado (CSR)

Uso openssl req -new para solicitar una .csr utilizando la clave privada y los archivos **.cnf** creados anteriormente

<#root>

```
Test-Laptop$
```

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

Uso ls -la para comprobar el cert.csr se crea.

<#root>

```
Test-Laptop$
```

ls -la | grep .csr

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

> **Nota**: si su organización utiliza una autoridad de certificación (CA), puede enviar esta CSR para obtener el certificado firmado por la CA.

Generar el archivo de certificado

Genere el .cer archivo con formato de código x509.

<#root>

```
Test-Laptop$
```

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

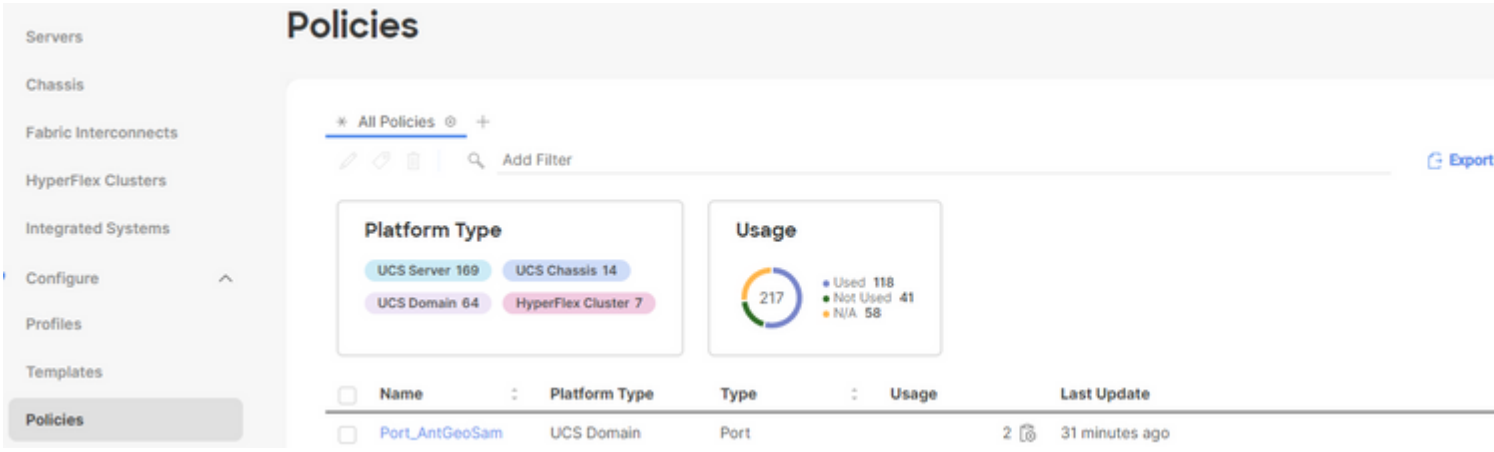
Uso ls -la para comprobar el certificate.cer se crea.

<#root>

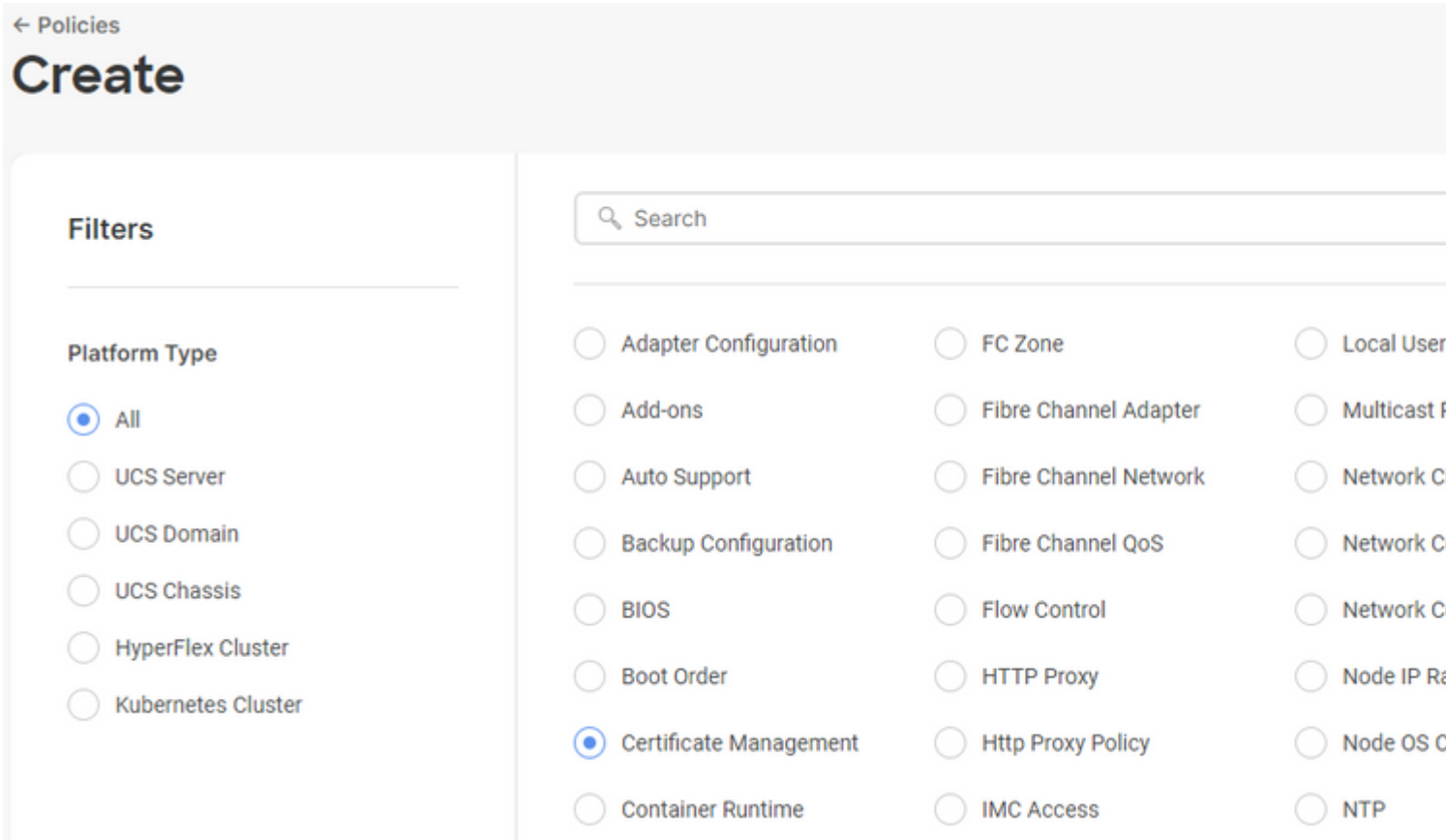
```
Test-Laptop$
ls -la | grep certificate.cer

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

Crear la directiva de administración de certificados en Intersight

Inicie sesión en su cuenta Intersight, navegue hasta Infrastructure Service, haga clic en la ficha Policies y haga clic en Create policy.



Filtre por servidor UCS y seleccione Administración de certificados.



Uso **cat** para copiar el contenido del certificado (certificate.cert) y el archivo de claves (cert.key) y péguelos en la directiva de administración de certificados en Intersight.

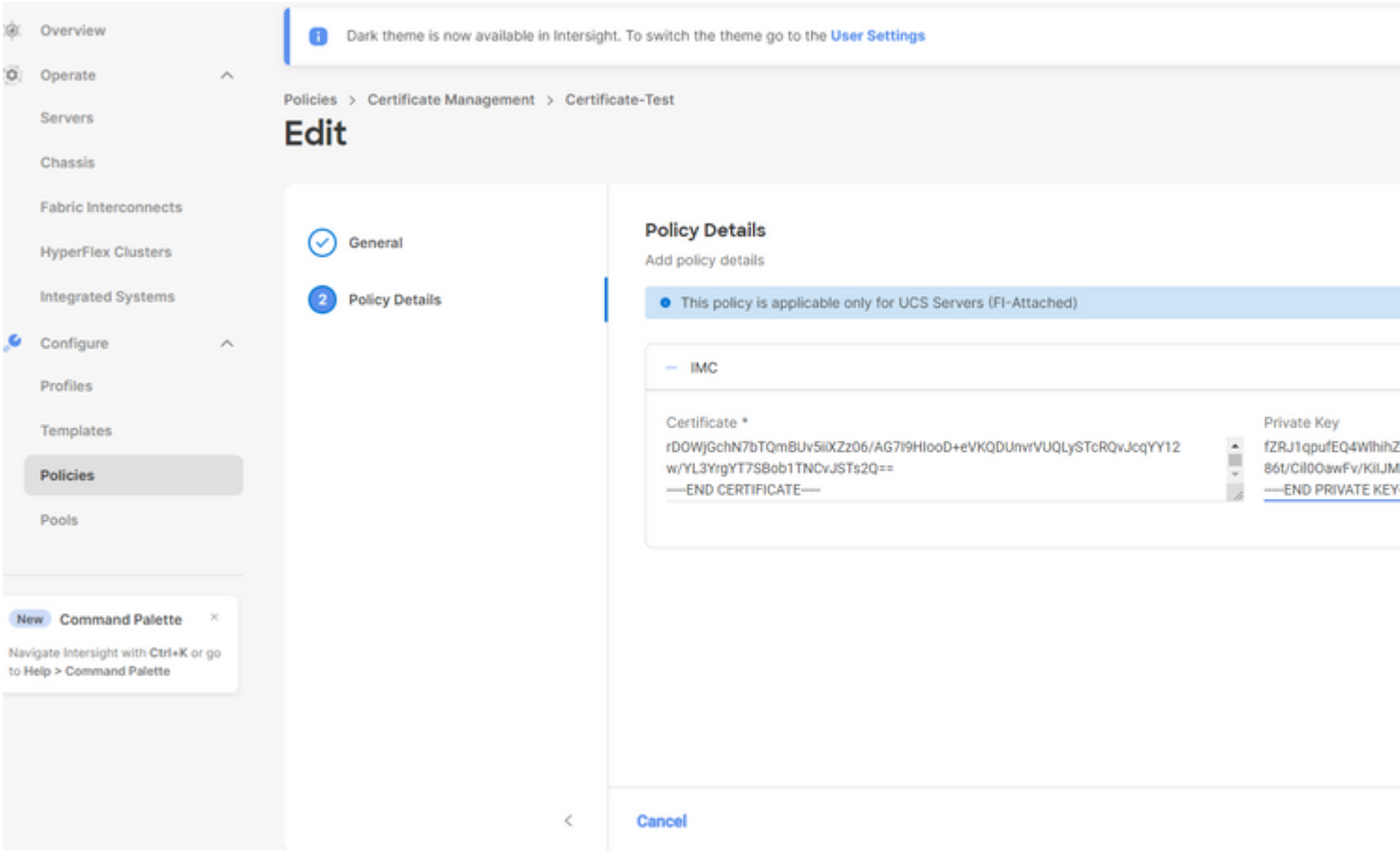
<#root>

```
Test-Laptop$
```

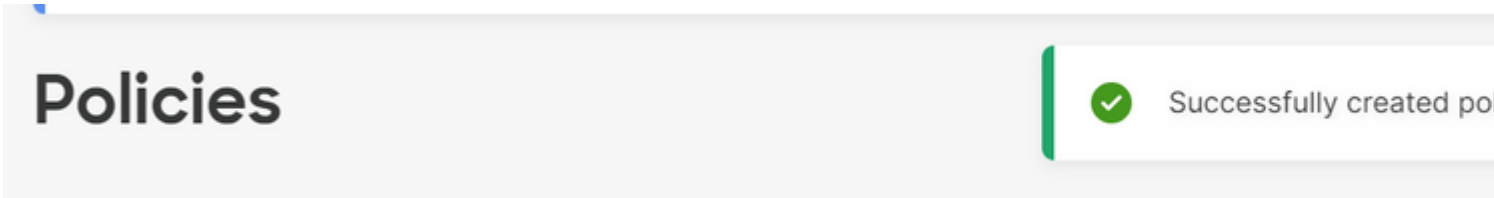
cat certificate.cert

```
Test-Laptop$
```

cat cert.key

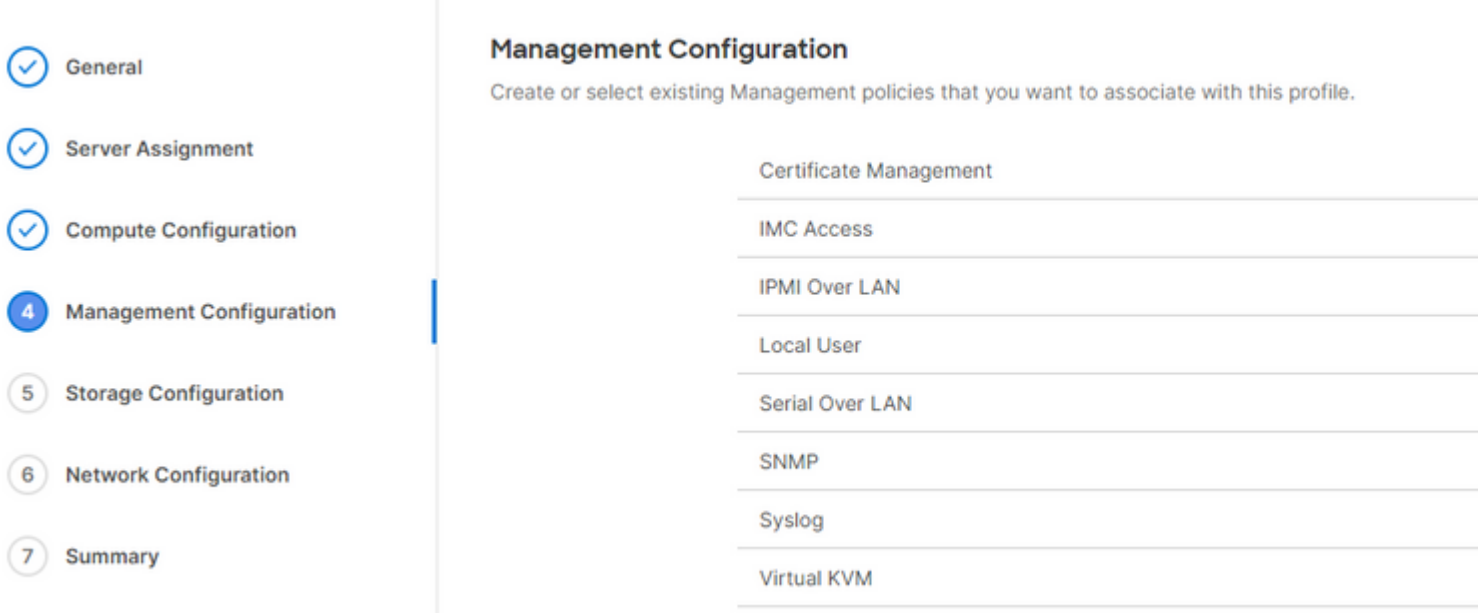


Compruebe que la directiva se ha creado sin errores.



Agregar la directiva a un perfil de servidor

Vaya a la ficha Profiles (Perfiles), modifique un perfil de servidor o cree un nuevo perfil y adjunte directivas adicionales si es necesario. En este ejemplo se modifica un perfil de servicio. Haga clic en editar y continuar, adjunte la directiva e implemente el perfil de servidor.



Troubleshoot

Si necesita verificar la información dentro de un certificado, CSR o clave privada, utilice estos comandos de OpenSSL:

Para comprobar los detalles de CSR:

<#root>

```
Test-Laptop$
```

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

Para comprobar los detalles del certificado:

<#root>

```
Test-Laptop$
```

openssl x509 -in cert.cer -text -noout

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).