Configura certificato per server gestiti da Intersight

Sommario

Introduzione

In questo documento viene descritto il processo di generazione di una richiesta CSR (Certificate Signed Request) per la creazione di certificati personalizzati per i server gestiti da Intersight.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Intersight
- Certificati di terze parti
- OpenSSL

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco UCS 6454 Fabric Interconnect, firmware 4.2(1m)
- Server blade UCSB-B200-M5, firmware 4.2(1c)
- SaaS (Intersight software as a service)

- Computer MAC con OpenSSL 1.1.1k

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In modalità Intersight Managed, i criteri di gestione dei certificati consentono di specificare i dettagli del certificato e della coppia di chiavi private per un certificato esterno e di allegare i criteri ai server. È possibile caricare e utilizzare lo stesso certificato esterno e la stessa coppia di chiavi private per più server gestiti Intersight.

Configurazione

In questo documento viene usato OpenSSL per generare i file necessari per ottenere la catena di certificati e la coppia di chiavi private.

Passaggio 1.	Creare la .cnf file contenente tutti i dettagli del certificato (deve includere gli indirizzi IP per la connessione IMC ai server).
Passaggio 2.	Creare la chiave privata e il .csr mediante OpenSSL.
Passaggio 3.	Inviare il file CSR a una CA per firmare il certificato. Se l'organizzazione genera certificati autofirmati, è possibile utilizzare il file CSR per generare un certificato autofirmato.
Passaggio 4.	Creare i criteri di gestione dei certificati in Intersight e incollare le catene Certificato e Coppia di chiavi privata.

Creazione del file di configurazione (.cnf)

Per creare il file di configurazione con l'estensione .cnf, utilizzate un editor di file. Specificare le impostazioni in base ai dettagli dell'organizzazione.

<#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

⚠ Attenzione: utilizzare i nomi soggetto alternativi per specificare ulteriori nomi host o indirizzi IP per i server. La mancata configurazione o l'esclusione dal certificato caricato può causare il blocco dell'accesso all'interfaccia Cisco IMC da parte dei browser.

Genera una chiave privata (.key)

Utilizzo `openssl genrsa` per generare una nuova chiave.

<#root>

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

Verificare il file denominato `cert.key` viene creato mediante `ls -la`

<#root>

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

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

Genera CSR

Utilizzo `openssl req -new` al fine di richiedere un `.csr` file utilizzando la chiave privata e `.cnf` file creati in precedenza.

<#root>

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

Utilizzo `ls -la` al fine di verificare la `cert.csr` viene creato.

<#root>

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

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

Nota: se l'organizzazione utilizza un'Autorità di certificazione (CA), è possibile inviare questo CSR per ottenere il certificato firmato dalla CA.

Genera il file di certificato

Genera il .cer file con formato codice x509.

<#root>

```
Test-Laptop$
```

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

Utilizzo ls -la al fine di verificare la certificate.cer viene creato.

<#root>

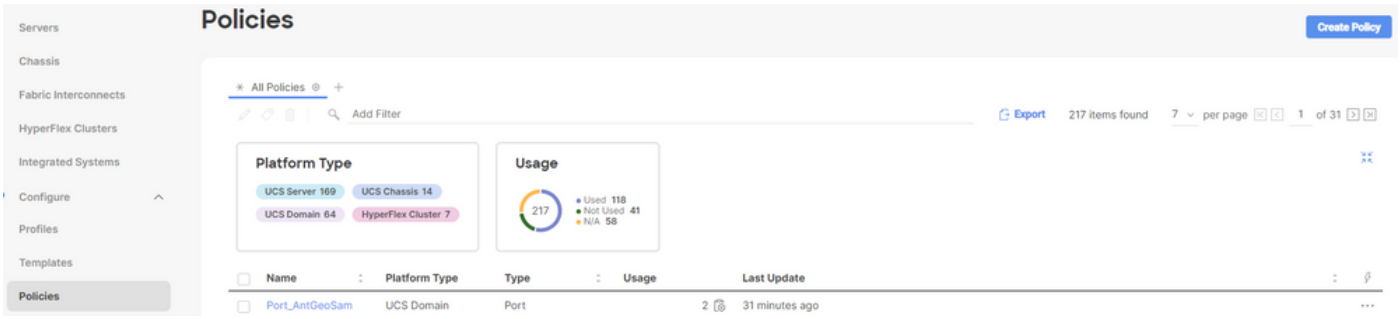
```
Test-Laptop$
```

ls -la | grep certificate.cer

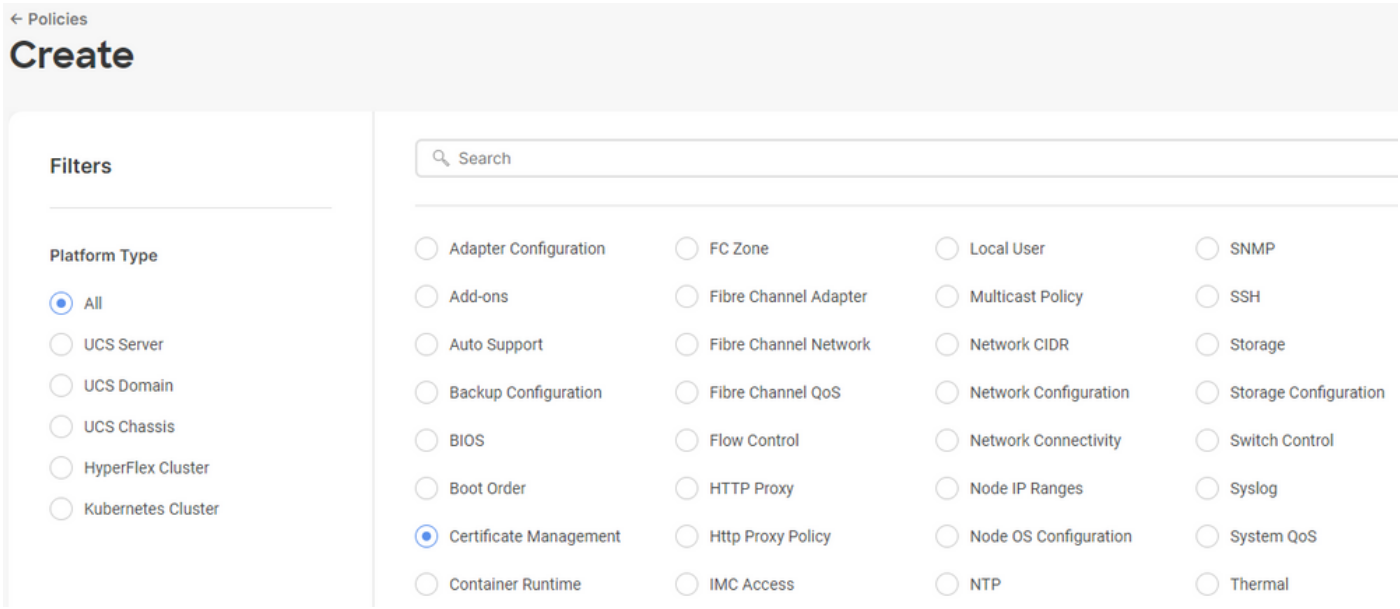
```
-rw-r--r-- 1 user staff 1090 Dec 13 21:54 certificate.cer
```

Creare i criteri di gestione dei certificati in Intersight

Accedere all'account Intersight, passare a Infrastructure Service, fare clic sul pulsante Policies , quindi fare clic su Create Policy.



Filtra per server UCS e scegli Certificate Management.



Utilizzare il **cat** Per copiare il contenuto del certificato (certificate.cert file) e il file di chiave (cert.key file) e incollarli in Certificate Management Policy in Intersight.

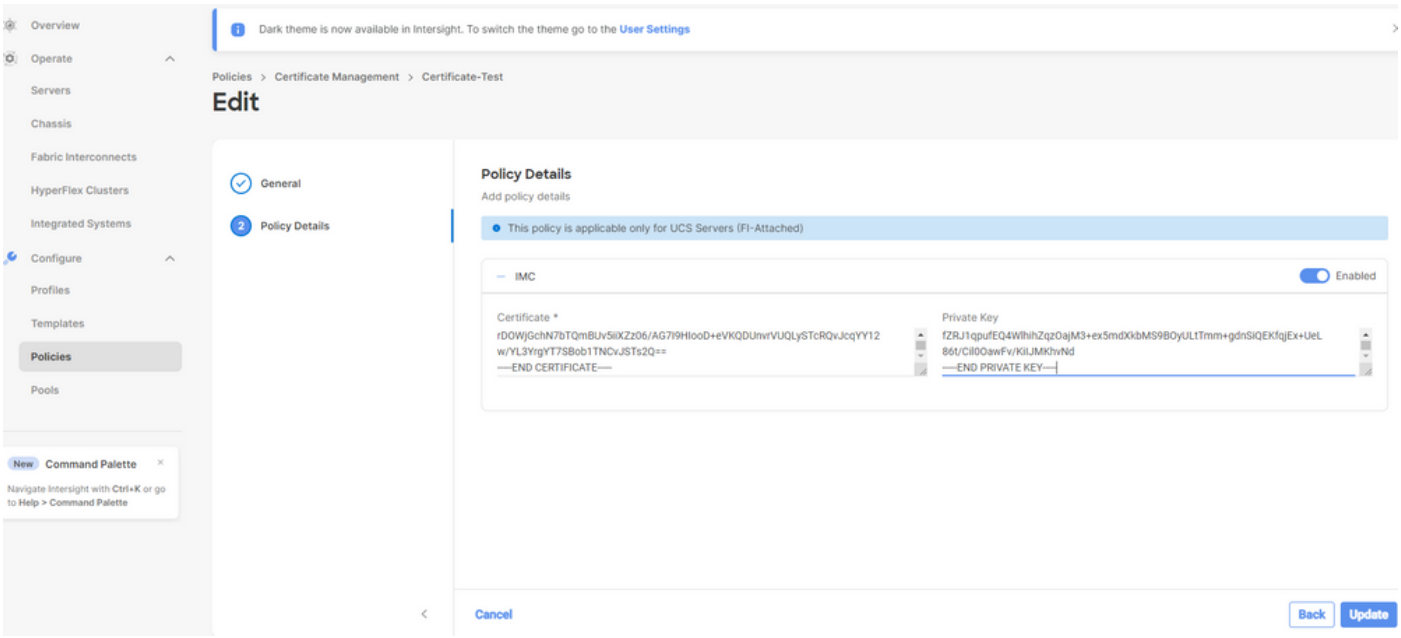
<#root>

Test-Laptop$

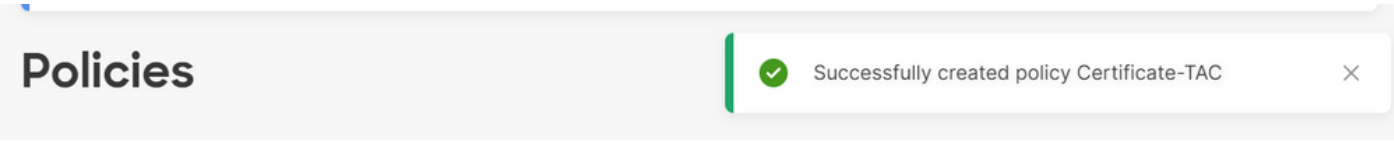
cat certificate.cert

Test-Laptop$

cat cert.key

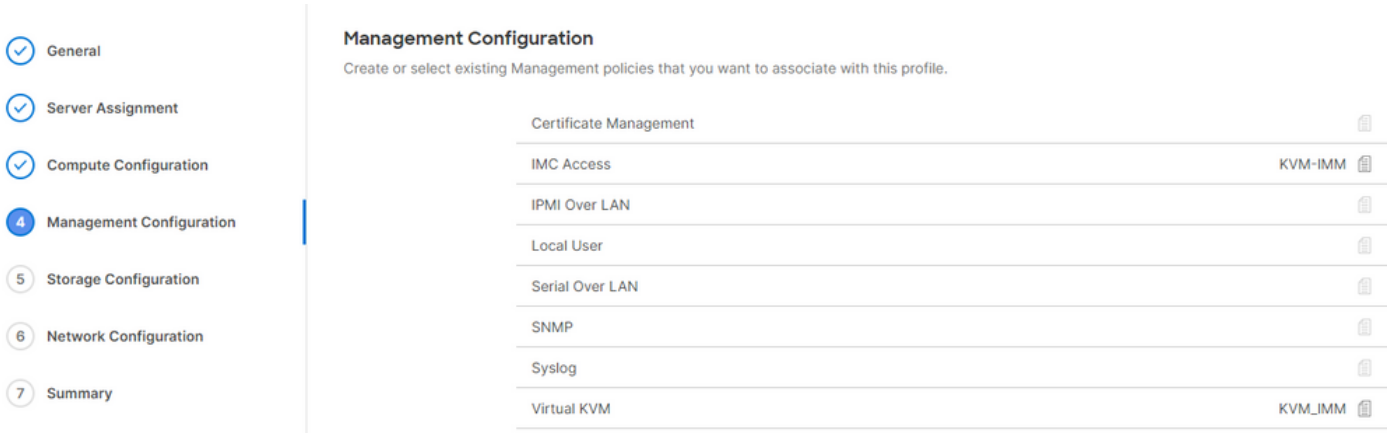


Verificare che il criterio sia stato creato senza errori.



Aggiungere il criterio a un profilo server

Passare alla Profiles e modificare un profilo server o creare un nuovo profilo e allegare criteri aggiuntivi, se necessario. In questo esempio viene modificato un profilo del servizio. Fare clic su edit e continuare, collegare il criterio e distribuire il profilo del server.



Risoluzione dei problemi

Se è necessario controllare le informazioni contenute in un certificato, in un CSR o in una chiave privata, utilizzare i comandi OpenSSL come indicato.

Per controllare i dettagli della CSR:

<#root>

```
Test-Laptop$
```

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

Per controllare i dettagli del certificato:

<#root>

```
Test-Laptop$
```

openssl x509 -in cert.cer -text -noout

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).