Zertifikat für von Intersight verwaltete Server konfigurieren

Inhalt

Einleitung

In diesem Dokument wird der Prozess zum Generieren einer mit einem Zertifikat signierten Anforderung beschrieben, um benutzerdefinierte Zertifikate für von Intersight verwaltete Server zu erstellen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Intersight
- Zertifikate von Drittanbietern
- OpenSSL

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco UCS 6454 Fabric Interconnect, Firmware 4.2(1 m)
- UCSB-B200-M5 Blade-Server, Firmware 4.2(1c)
- Intersight Software-as-a-Service (SaaS)
- MAC-Computer mit OpenSSL 1.1.1k

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Im intersight Managed Mode können Sie mit der Zertifikatverwaltungsrichtlinie das Zertifikat und die Details des privaten Schlüsselpaars für ein externes Zertifikat angeben und die Richtlinie an die Server anhängen. Sie können dasselbe externe Zertifikat und dasselbe private Schlüsselpaar für mehrere Intersight Managed Server hochladen und verwenden.

Konfigurieren

In diesem Dokument wird OpenSSL verwendet, um die Dateien zu generieren, die zum Abrufen der Zertifikatkette und des privaten Schlüsselpaars erforderlich sind.

Schritt 1:	Erstellen Sie die CNF-Datei, die alle Details des Zertifikats enthält (sie muss die IP-Adressen für die IMC-Verbindung zu den Servern enthalten).
Schritt 2:	Erstellen Sie den privaten Schlüssel und die CSR-Dateien über OpenSSL.
Schritt 3:	Senden Sie die CSR-Datei an eine Zertifizierungsstelle, um das Zertifikat zu signieren. Wenn Ihre Organisation ihre eigenen selbstsignierten Zertifikate generiert, können Sie die CSR-Datei verwenden, um ein selbstsigniertes Zertifikat zu generieren.
Schritt 4:	Erstellen Sie die Zertifikatverwaltungsrichtlinie in Intersight, und fügen Sie die Zertifikatsketten und die privaten Schlüsselpaarketten ein.

Erstellen der Konfigurationsdatei (.cnf)

Verwenden Sie einen Datei-Editor, um die Konfigurationsdatei mit der Erweiterung **.cnf** zu erstellen. Füllen Sie die Einstellungen basierend auf Ihren Organisationsdetails aus.

<#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
```

> **Vorsicht**: Verwenden Sie die *alternativen Antragstellernamen*, um zusätzliche Hostnamen oder IP-Adressen für Ihre Server anzugeben. Wird das Zertifikat nicht konfiguriert oder vom hochgeladenen Zertifikat ausgeschlossen, kann dies dazu führen, dass Browser den Zugriff auf die Cisco IMC-Schnittstelle blockieren.

Generieren eines privaten Schlüssels (.key)

Verwenden Sie **openssl genrsa**, um einen neuen Schlüssel zu generieren.

```
<#root>

Test-Laptop$

openssl genrsa -out cert.key 2048
```

Überprüfen Sie die Datei mit dem Namen cert.key wird mithilfe des ls -la aus.

<#root>

```
Test-Laptop$
```

ls -la | grep cert.key

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

CSR (Certificate Signed Request) generieren

Nutzung openssl req -new um eine .csr -Datei mit dem privaten Schlüssel und **.cnf**-Dateien, die zuvor erstellt wurden

<#root>

```
Test-Laptop$
```

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

Nutzung ls -la zur Überprüfung der cert.csr wird erstellt.

<#root>

```
Test-Laptop$
```

ls -la | grep .csr

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

> **Hinweis**: Wenn Ihre Organisation eine Zertifizierungsstelle verwendet, können Sie diese CSR-Anfrage einreichen, um das Zertifikat von Ihrer Zertifizierungsstelle signieren zu lassen.

Zertifikatsdatei generieren

Generieren Sie die .cer Datei im x509-Codeformat.

<#root>

```
Test-Laptop$
```

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

Nutzung ls -la zur Überprüfung der certificate.cer wird erstellt.

<#root>

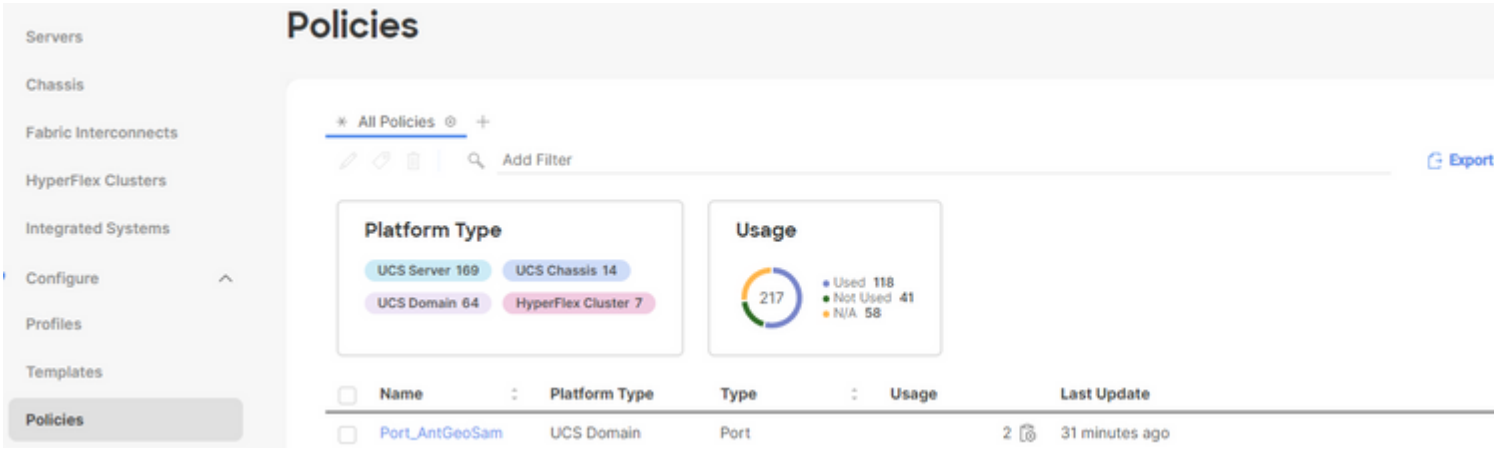
```
Test-Laptop$
```

`ls -la | grep certificate.cer`

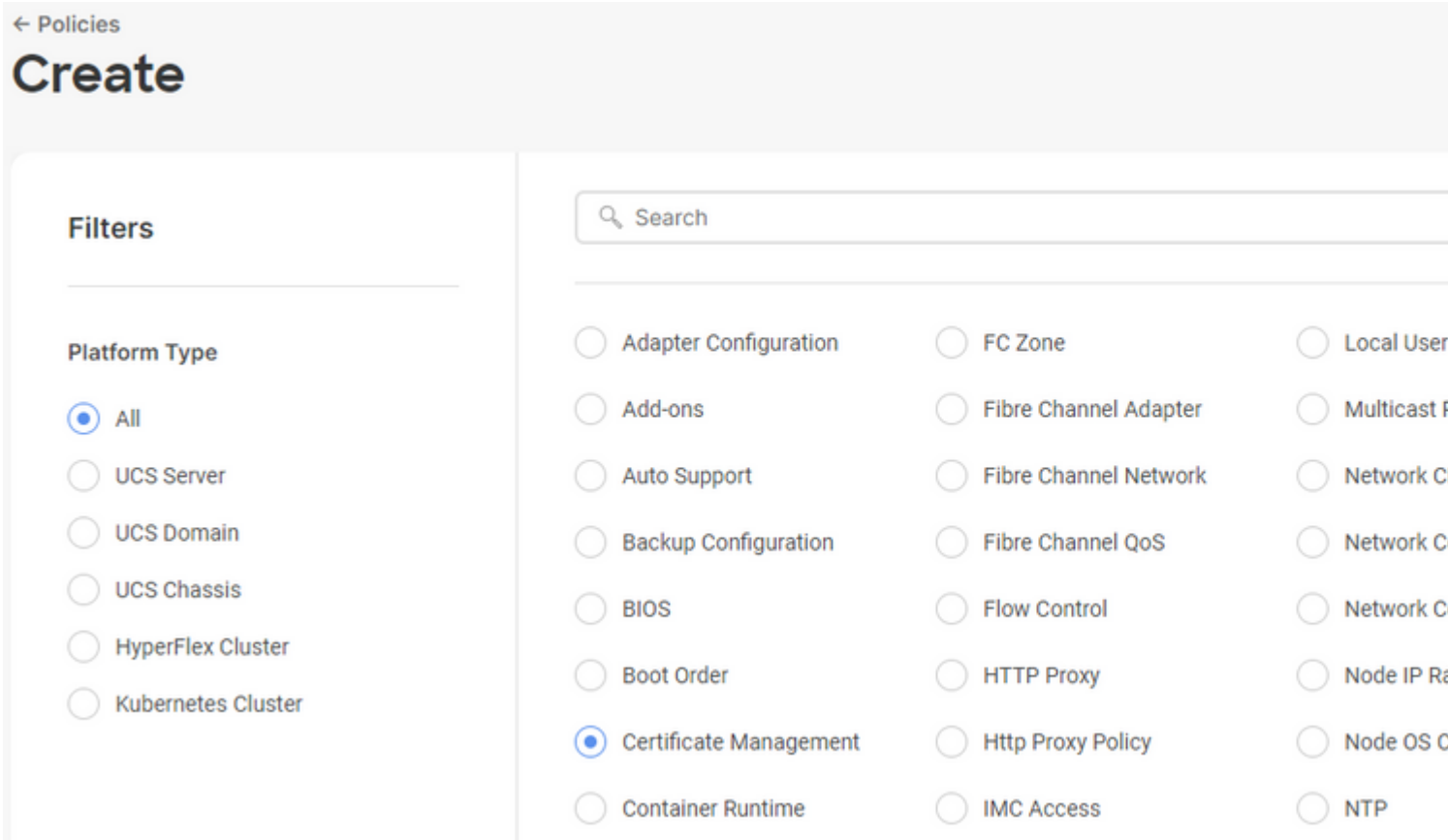
```
-rw-r--r-- 1 user staff 1090 Dec 13 21:54 certificate.cer
```

Zertifikatverwaltungsrichtlinie in Intersight erstellen

Melden Sie sich bei Ihrem Intersight-Konto an, navigieren Sie zu Infrastructure Service, klicken Sie auf die Registerkarte Policies (Richtlinien), und klicken Sie auf Create policy (Richtlinie erstellen).



Filtern Sie nach UCS Server, und wählen Sie Certificate Management aus.



Nutzung **cat** -Befehl, um den Inhalt des Zertifikats (certificate.cert Datei) und die Schlüsseldatei (cert.key Datei) und fügen Sie sie in Intersight in die Richtlinie zur Zertifikatsverwaltung ein.

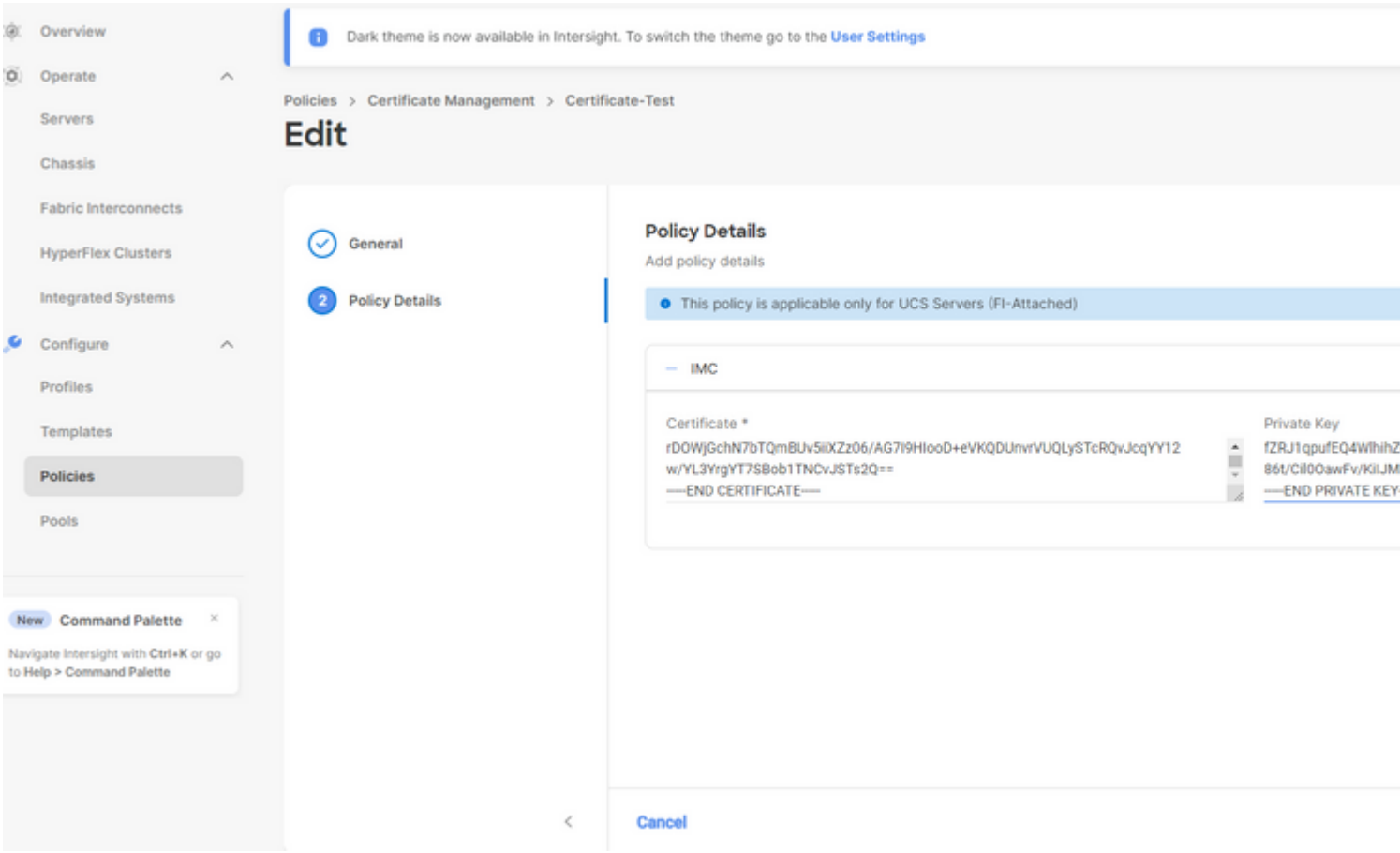
<#root>

```
Test-Laptop$
```

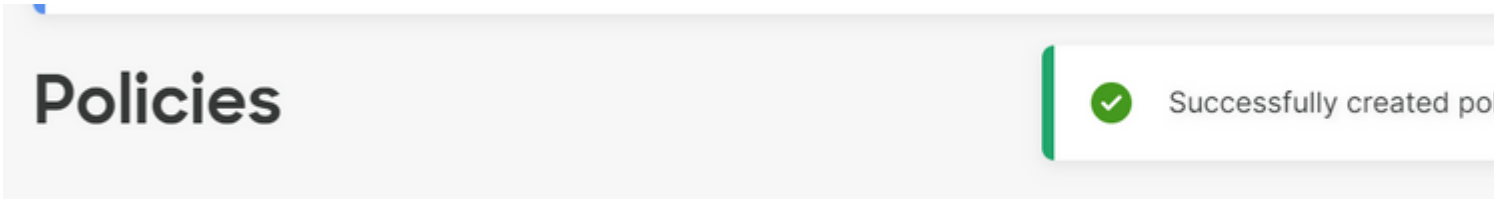
```
cat certificate.cert
```

```
Test-Laptop$
```

```
cat cert.key
```

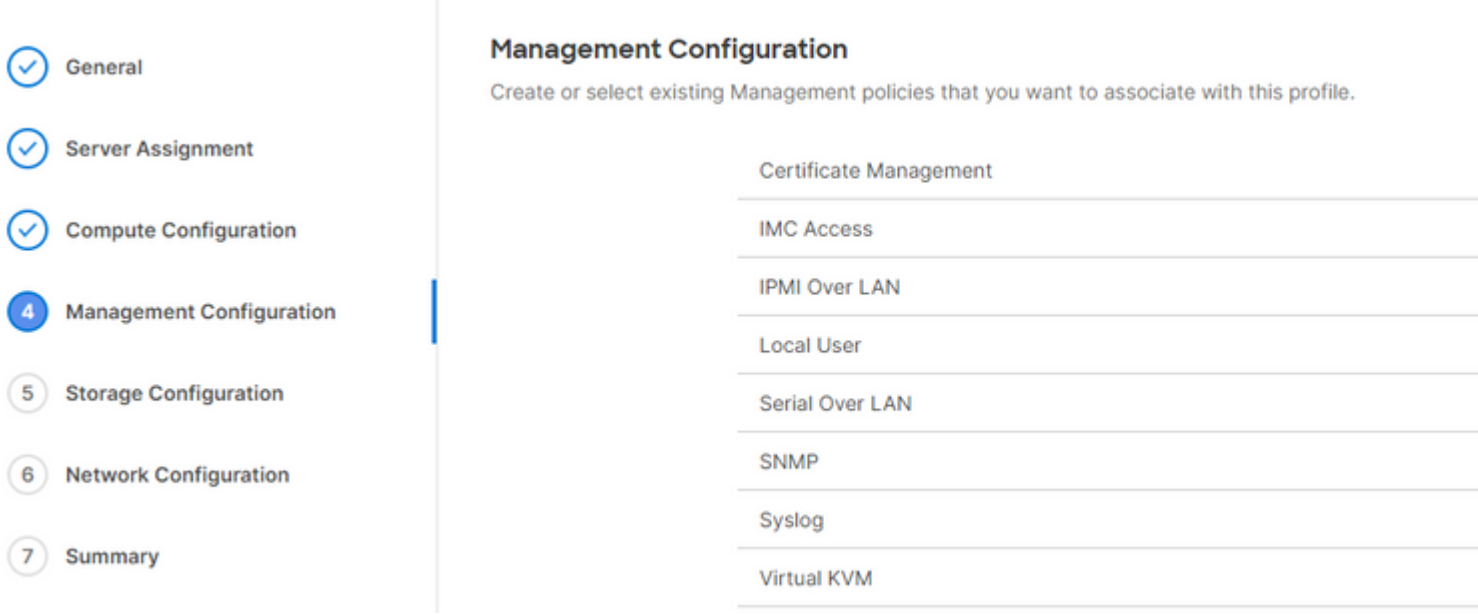


Überprüfen, ob die Richtlinie fehlerfrei erstellt wurde



Richtlinie einem Serverprofil hinzufügen

Navigieren Sie zur Registerkarte Profiles (Profile), ändern Sie ein Serverprofil, erstellen Sie ein neues Profil, und hängen Sie ggf. zusätzliche Richtlinien an. In diesem Beispiel wird ein Serviceprofil geändert. Klicken Sie auf "Bearbeiten und fortfahren", hängen Sie die Richtlinie an, und stellen Sie das Serverprofil bereit.



Fehlerbehebung

Wenn Sie die Informationen in einem Zertifikat, CSR oder privaten Schlüssel überprüfen müssen, verwenden Sie die folgenden OpenSSL-Befehle:

So überprüfen Sie die CSR-Details:

<#root>

```
Test-Laptop$
```

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

So überprüfen Sie Zertifikatdetails:

<#root>

```
Test-Laptop$
```

openssl x509 -in cert.cer -text -noout

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.