# Zertifikat für von Intersight verwaltete Server konfigurieren

# Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren CSR (Certificate Signed Request) generieren Schlüsseldatei generieren Zertifikatverwaltungsrichtlinie in Intersight erstellen Richtlinie einem Serverprofil hinzufügen

## 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 verstehen.

## 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.

## Konfigurieren

#### CSR (Certificate Signed Request) generieren

Test-Laptop\$ openssl req -new > intersight.ssl.csr

Nutzung openssi req -new und die Ausgabe an eine .csr Datei. Geben Sie die Einstellungen für Ihre Organisation ein.

Generating a RSA private key ....+++++ ....++++++ writing new private key to 'privkey.pem' Enter PEM pass phrase: Verifying - Enter PEM pass phrase: You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [AU]:MEX string is too long, it needs to be no more than 2 bytes long Country Name (2 letter code) [AU]:MX State or Province Name (full name) [Some-State]:MX Locality Name (eg, city) []:MX Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Organizational Unit Name (eg, section) []:TAC Common Name (for example server FQDN or YOUR name) []:ESX01PROD Email Address []:ip-operationgroup@cisco.com

Please enter these 'extra' attributes
to be sent with your certificate request
A challenge password []:Cisco123!
An optional company name []:Cisco123!

Hinweis: Einige Felder sind optional.

Nutzung Is -la zur Überprüfung der intersight.ssl.csr und privkey.pem Dateien erstellt werden.

Test-Laptop\$ **ls -la | grep .pem** -rw----- 1 user staff 1854 Dec 13 21:52 privkey.pem

## Schlüsseldatei generieren

```
Test-Laptop$ openssl rsa -in privkey.pem -out new.cert.key
Enter pass phrase for privkey.pem:
writing RSA key
```

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

```
Test-Laptop$ 1s -1a | grep new.cert.key
-rw----- 1 user staff 1675 Dec 13 21:59 new.cert.key
```

Generieren Sie die .cert Datei im x509-Codeformat.

```
Test-Laptop$ openssl x509 -in intersight.ssl.csr -out intersight.cert.cert -req -signkey
new.cert.key -days 4000
Signature ok
subject=C = MX, ST = MX, L = MX, O = Cisco, OU = TAC, CN = SV, emailAddress = ip-
operationgroup@cisco.com
Getting Private key
```

#### 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).

Servers	Policies		Create Policy
Chassis			
Fabric Interconnects	* All Policies  +		
HyperFlex Clusters		217 items found	7 ∨ per page K < 1 of 31 > >
Integrated Systems	Platform Type Usage		38
Configure ^	UCS Server 109 UCS Chassis 14 . Used 118		
Profiles	UCS Domain 64 HyperFlex Cluster 7 • Not Used 41 • N/A 58		
Templates	Name : Platform Type : Usage Last Update		: Ø
Policies	Port 2 1 3 31 minutes ago		

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

<ul><li>← Policies</li><li>Create</li></ul>				
Filters	Q, Search			
Platform Type	Adapter Configuration	O FC Zone	C Local User	SNMP
<ul> <li>All</li> </ul>	Add-ons	Fibre Channel Adapter	Multicast Policy	SSH
UCS Server	Auto Support	Fibre Channel Network	Network CIDR	Storage
UCS Domain	Backup Configuration	Fibre Channel QoS	Network Configuration	Storage Configuration
UCS Chassis	BIOS	Flow Control	Network Connectivity	Switch Control
HyperFlex Cluster	O Boot Order	HTTP Proxy	Node IP Ranges	Syslog
U Kubernetes Cluster	<ul> <li>Certificate Management</li> </ul>	Http Proxy Policy	Node OS Configuration	System QoS
	O Container Runtime	IMC Access		Thermal

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

Test-Laptop\$ cat intersight.cer	t.cert
Test-Laptop\$ cat new.cert.key	
Overview     Overview     Dark theme is now available in Intersig	ght. To switch the theme go to the User Settings
Operate     Policies > Certificate Management > Certi     Certi     Chassis	ficate-Test
Fabric Interconnects       HyperFlex Clusters       Integrated Systems       Integrated Systems	Policy Details Add policy details • This policy is applicable only for UCS Servers (FI-Attached)
Configure	- IMC Enabled
Templates Policies Pools	Certificate * Private Key r00WjGchN7bTQmBU/SIXZ206/AG7I9HI00D+eVKQDUmv/VUQLySTCRQvJcqYY12 w/YL3YrgYT7SBob1TNCvJSTs2Q== - END PRIVATE KEY
New Command Palette × Navigate Intersight with Ctrl+K or go to Help > Command Palette	
	Cancel Back Update

Überprüfen, ob die Richtlinie fehlerfrei erstellt wurde



## Richtlinie einem Serverprofil hinzufügen

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

#### Management Configuration

Create or select existing Management policies that you want to associate with this profile.

$\bigcirc$	Server Assignment	Server Assignment	
$\smile$			

- Compute Configuration
- Management Configuration
- 5 Storage Configuration
- 6 Network Configuration
- 7 Summary

 Certificate Management

 IMC Access

 IPMI Over LAN

 Local User

 Serial Over LAN

 SNMP

 Syslog

 Virtual KVM

## 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.