

Intersight에서 관리하는 서버에 대한 인증서 구성

목차

- [소개](#)
- [사전 요구 사항](#)
 - [요구 사항](#)
 - [사용되는 구성 요소](#)
- [배경 정보](#)
- [구성](#)
 - [구성 파일\(.cnf\) 만들기](#)
 - [개인 키\(.key\) 생성](#)
 - [CSR 생성](#)
 - [인증서 파일 생성](#)
 - [Intersight에서 인증서 관리 정책 생성](#)
 - [서버 프로필에 정책 추가](#)
- [문제 해결](#)

소개

이 문서에서는 Intersight에서 관리하는 서버에 대해 사용자 지정된 인증서를 만들기 위해 CSR(Certificate Signed Request)을 생성하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Intersight
- 서드파티 인증서
- OpenSSL

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco UCS 6454 Fabric Interconnect, 펌웨어 4.2(1m)
- UCSB-B200-M5 블레이드 서버, 펌웨어 4.2(1c)
- Intersight SaaS(Software as a Service)
- OpenSSL 1.1.1k를 사용하는 MAC 컴퓨터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Intersight Managed Mode에서 Certificate Management(인증서 관리) 정책을 사용하면 외부 인증서에 대한 인증서 및 개인 키 쌍 세부 정보를 지정하고 서버에 정책을 연결할 수 있습니다. 여러 Intersight Managed Server에 동일한 외부 인증서 및 개인 키 쌍을 업로드하고 사용할 수 있습니다.

구성

이 문서에서는 OpenSSL을 사용하여 인증서 체인 및 개인 키 쌍을 가져오는 데 필요한 파일을 생성합니다.

1단계.	Create(생성) .cnf 인증서의 모든 세부사항이 있는 파일(서버에 대한 IMC 연결을 위한 IP 주소를 포함해야 함)
2단계.	개인 키 및 .csr OpenSSL을 통한 파일
3단계.	인증서를 서명하려면 CSR 파일을 CA에 제출합니다. 조직에서 자체 서명 인증서를 생성하는 경우 CSR 파일을 사용하여 자체 서명 인증서를 생성할 수 있습니다.
4단계.	Intersight에서 인증서 관리 정책을 생성하고 인증서 및 개인 키 쌍 체인을 붙여넣습니다.

구성 파일(.cnf) 만들기

확장명이 .cnf인 컨피그레이션 파일을 만들려면 파일 편집기를 사용합니다. 조직 세부사항에 따라 설정을 입력합니다.

```
<#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



주의: Subject Alternate Name(주체 대체 이름)을 사용하여 서버에 대한 추가 호스트 이름 또는 IP 주소를 지정합니다. 이를 구성하지 않거나 업로드된 인증서에서 제외하면 브라우저에서 Cisco IMC 인터페이스에 대한 액세스를 차단할 수 있습니다.

개인 키(.key) 생성

Use `openssl genrsa` 새 키를 생성합니다.

```
<#root>
```

```
Test-Laptop$
```

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

이름이 인 파일을 확인합니다. `cert.key` 이(가) `ls -la` 명령을 실행합니다.

```
<#root>
```

```
Test-Laptop$
```

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

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

CSR 생성

Use `openssl req -new` 요청을 하려면 `.csr` 개인 키 및 `.cnf` 이전에 만든 파일입니다.

```
<#root>
```

```
Test-Laptop$
```

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


Use `ls -la` 을(를) 검증하려면 `cert.csr` 이(가) 생성됩니다.

```
<#root>
```

```
Test-Laptop$
```

```
ls -la | grep .csr
```

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

 참고: 조직에서 CA(Certificate Authority)를 사용하는 경우 CA에서 서명한 인증서를 가져오기 위해 이 CSR을 제출할 수 있습니다.

인증서 파일 생성

생성 .cer x509 코드 형식의 파일입니다.

```
<#root>
```

```
Test-Laptop$
```

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

Use `ls -la` 을(를) 검증하려면 `certificate.cer` 이(가) 생성됩니다.

```
<#root>
```

```
Test-Laptop$
```

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

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

Intersight에서 인증서 관리 정책 생성

Intersight 계정에 로그인하고 Infrastructure Service을 클릭하고 Policies 탭을 클릭한 다음 Create Policy.

Name	Platform Type	Type	Usage	Last Update
<input type="checkbox"/> Port_AntGeoSam	UCS Domain	Port	2	31 minutes ago

UCS Server로 필터링하고 Certificate Management.

Create

Filters

Platform Type

- All
- UCS Server
- UCS Domain
- UCS Chassis
- HyperFlex Cluster
- Kubernetes Cluster

Search

- Adapter Configuration
- Add-ons
- Auto Support
- Backup Configuration
- BIOS
- Boot Order
- Container Runtime
- Certificate Management
- FC Zone
- Fibre Channel Adapter
- Fibre Channel Network
- Fibre Channel QoS
- Flow Control
- HTTP Proxy
- Http Proxy Policy
- IMC Access
- Local User
- Multicast Policy
- Network CIDR
- Network Configuration
- Network Connectivity
- Node IP Ranges
- Node OS Configuration
- NTP
- SNMP
- SSH
- Storage
- Storage Configuration
- Switch Control
- Syslog
- System QoS
- Thermal

이 `cat` 명령 인증서의 내용(`certificate.cert` 파일) 및 키 파일(`cert.key`) Intersight의 인증서 관리 정책에 붙여넣습니다.

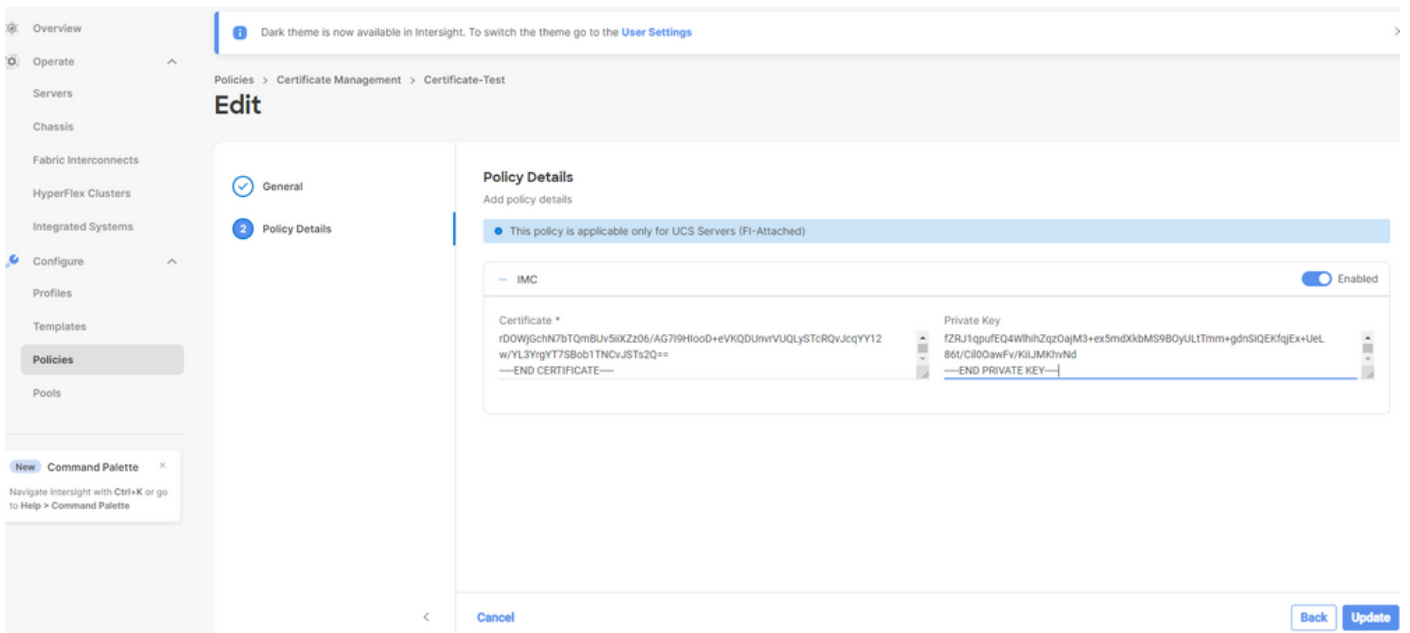
```
<#root>
```

```
Test-Laptop$
```

```
cat certificate.cert
```

```
Test-Laptop$
```

```
cat cert.key
```



정책이 오류 없이 생성되었는지 확인합니다.

Policies



Successfully created policy Certificate-TAC



서버 프로필에 정책 추가

탐색: Profiles 서버 프로필을 탭하여 수정하거나 새 프로필을 만들고 필요한 경우 추가 정책을 첨부합니다. 이 예에서는 서비스 프로필을 수정합니다. 클릭 edit 계속 진행하여 정책을 어태치하고 서버 프로필을 구축합니다.

- General
- Server Assignment
- Compute Configuration
- 4 Management Configuration**
- 5 Storage Configuration
- 6 Network Configuration
- 7 Summary

Management Configuration

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

Certificate Management	
IMC Access	KVM-IMM
IPMI Over LAN	
Local User	
Serial Over LAN	
SNMP	
Syslog	
Virtual KVM	KVM_IMM

문제 해결

Certificate(인증서), CSR 또는 Private Key(개인 키) 내의 정보를 확인해야 하는 경우, 앞서 설명한 대로 OpenSSL 명령을 사용합니다.

CSR 세부사항을 확인하려면 다음을 수행합니다.

```
<#root>
```

```
Test-Laptop$
```

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

인증서 세부사항을 확인하려면 다음을 수행합니다.

```
<#root>
```

```
Test-Laptop$
```

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.