

Intersightによって管理されるサーバの証明書の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[コンフィギュレーションファイル\(.cnf\)の作成](#)

[秘密キー\(.key\)の生成](#)

[CSRの生成](#)

[証明書ファイルの生成](#)

[Intersightでの証明書管理ポリシーの作成](#)

[サーバプロファイルへのポリシーの追加](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Intersightが管理するサーバ用にカスタマイズされた証明書を作成するための証明書署名要求(CSR)を生成するプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Intersight
- サードパーティ証明書
- OpenSSL

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco UCS 6454ファブリックインターコネクト、ファームウェア4.2(1m)
- UCSB-B200-M5ブレードサーバ、ファームウェア4.2(1c)
- Intersight Software as a Service(SaaS)
- OpenSSL 1.1.1kを使用するMACコンピュータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Intersight管理モードでは、証明書管理ポリシーを使用して、外部証明書の証明書と秘密キーペアの詳細を指定し、ポリシーをサーバに適用できます。複数のIntersight管理対象サーバに同じ外部証明書と秘密キーペアをアップロードして使用できます。

設定

このドキュメントでは、証明書チェーンと秘密キーペアを取得するために必要なファイルを生成するためにOpenSSLを使用します。

| | |
|------------|---|
| ステップ 1: | 新しい .cnf 証明書のすべての詳細を含むファイル（サーバへのIMC接続のIPアドレスを含む必要があります）。 |
| ステップ 2. | 秘密キーと .csr OpenSSLを介したファイル。 |
| 手順 3: | CSRファイルをCAに送信して、証明書に署名します。組織が独自の自己署名証明書を生成する場合は、CSRファイルを使用して自己署名証明書を生成できます。 |
| ステップ 4: | Intersightで証明書管理ポリシーを作成し、証明書と秘密キーペアのチェーンを貼り付けます。 |

コンフィギュレーションファイル(.cnf)の作成

ファイルエディタを使用して、.cnf拡張子を持つコンフィギュレーションファイルを作成します。組織の詳細に基づいて設定を入力します。

```
<#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
```

 注意：サブジェクトの別名(SAN)を使用して、サーバの追加のホスト名またはIPアドレスを

 指定してください。設定しないか、アップロードされた証明書から除外すると、ブラウザが Cisco IMC インターフェイスへのアクセスをブロックする可能性があります。

秘密キー(.key)の生成

利用 `openssl genrsa` 新しいキーを生成します。

```
<#root>
```

```
Test-Laptop$
```

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

という名前のファイルを確認します。 `cert.key` 作成されます。 `ls -la` コマンドを使用して、アップグレードを実行します。

```
<#root>
```

```
Test-Laptop$
```

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

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

CSR の生成

利用 `openssl req -new` IPアドレスを要求するために、 `.csr` 秘密キーを使用し、 `.cnf` ファイルを作成します。

```
<#root>
```

```
Test-Laptop$
```

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


利用 `ls -la` この設定を確認するには、 `cert.csr` 作成されます。

```
<#root>
```

```
Test-Laptop$
```

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

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

 注：組織で認証局(CA)を使用している場合は、このCSRを送信して、CAによって署名された証明書を取得できます。

証明書ファイルの生成

生成：.cer x509コード形式のファイル。

```
<#root>
```

```
Test-Laptop$
```

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

利用 `ls -la` この設定を確認するには、`certificate.cer` 作成されます。

```
<#root>
```

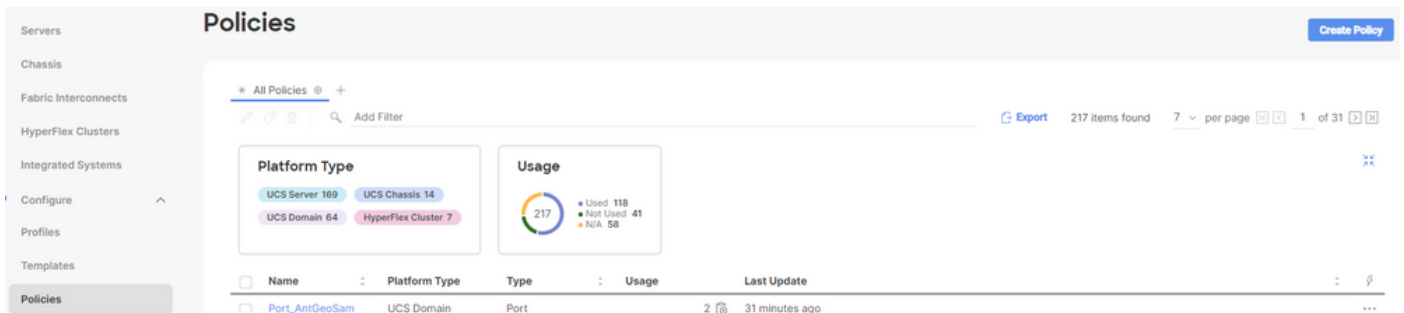
```
Test-Laptop$
```

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

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

Intersightでの証明書管理ポリシーの作成

Intersightアカウントにログインし、Infrastructure Service,ポリシーの横の [レポート (report)] Policies タブをクリックし、Create Policyを参照。



| Name | Platform Type | Type | Usage | Last Update |
|----------------|---------------|------|-------|----------------|
| Port_AntGeoSam | UCS Domain | Port | 2 | 31 minutes ago |

UCSサーバでフィルタリングし、Certificate Managementを参照。

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
- Certificate Management
- Container Runtime
- 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

cat コマンドを発行して、証明書(certificate.cert ファイル)およびキーファイル(cert.key ファイルに保存)し、Intersightの証明書管理ポリシーに貼り付けます。

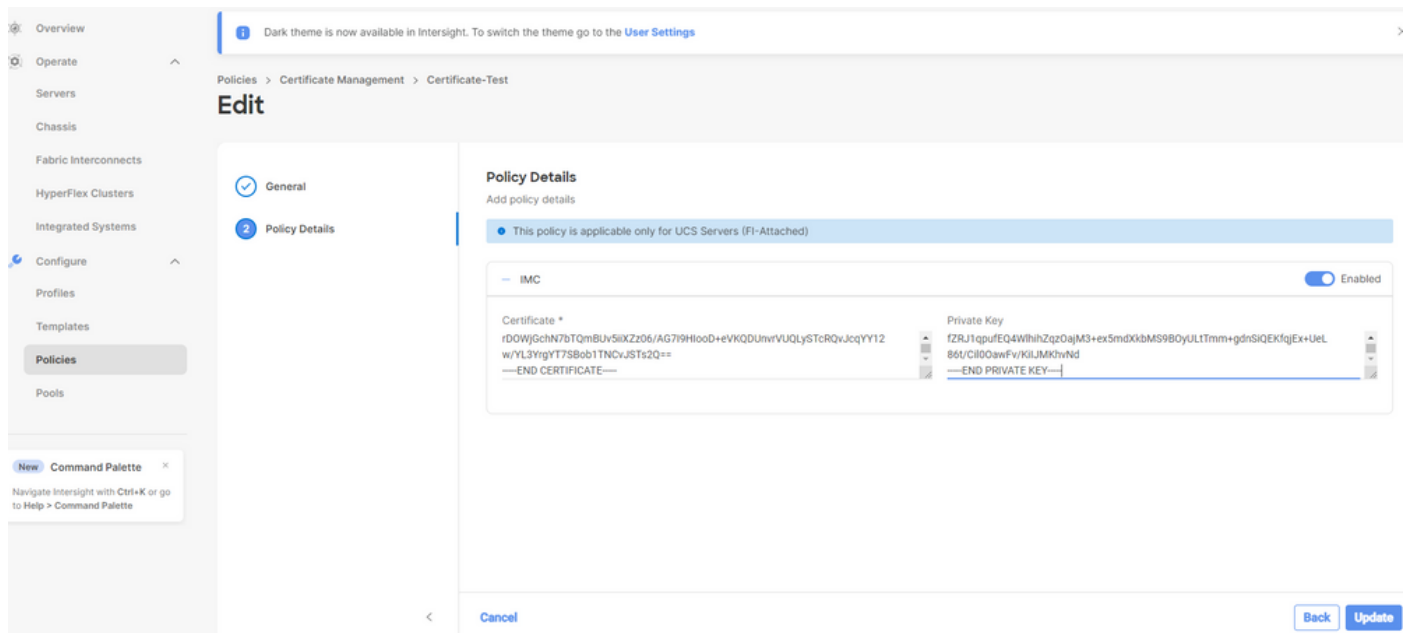
```
<#root>
```

```
Test-Laptop$
```

```
cat certificate.cert
```

```
Test-Laptop$
```

```
cat cert.key
```



ポリシーがエラーなしで作成されていることを確認します。

Policies

✓ Successfully created policy Certificate-TAC



サーバプロファイルへのポリシーの追加

次に移動します。 Profiles タブをクリックしてサーバプロファイルを変更するか、新しいプロファイルを作成し、必要に応じて追加のポリシーを適用します。この例では、サービスプロファイルを変更します。クリック edit 続行し、ポリシーを添付して、サーバプロファイルを導入します。

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 |

トラブルシューティング

証明書、CSR、または秘密キー内の情報を確認する必要がある場合は、前述のようにOpenSSLコマンドを使用します。

CSRの詳細を確認するには、次の手順を実行します。

```
<#root>
```

```
Test-Laptop$
```

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

証明書の詳細を確認するには、次のようにします。

```
<#root>
```

```
Test-Laptop$
```

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。