為Intersight管理的伺服器配置證書

目錄

<u>簡介</u>
<u>必要條件</u>
<u>需求</u>
採用元件
<u>背景資訊</u>
<u>設定</u>
<u>建立配置檔案(.cnf)</u>
<u>生成私鑰(.key)</u>
<u>產生CSR</u>
<u>生成證書檔案</u>
在Intersight中建立證書管理策略
<u>將策略新增到伺服器配置檔案</u>
疑難排解

簡介

本檔案介紹產生憑證簽署請求(CSR)的流程,以為Intersight管理的伺服器建立自訂憑證。

必要條件

需求

思科建議您瞭解以下主題:

- Intersight
- 第三方證書
- OpenSSL

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco UCS 6454交換矩陣互聯,韌體4.2(1m)
- UCSB-B200-M5刀鋒伺服器,韌體4.2(1c)
- Intersight軟體即服務(SaaS)
- 採用OpenSSL 1.1.1k的MAC電腦

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

在Intersight託管模式下,證書管理策略允許您為外部證書指定證書和私鑰對詳細資訊並將策略附加 到伺服器。您可以為多個Intersight託管伺服器上傳和使用相同的外部證書和私鑰對。

設定

本檔案使用OpenSSL來產生取得憑證鏈結和私密金鑰配對所需的檔案。

步驟	建立 .cnf 包含證書的所有詳細資訊的檔案(它必須包含用於與伺服器的IMC連線的IP地址
1.)。
步驟 2.	建立私鑰和 .csr 通過OpenSSL上傳檔案。
步驟	將CSR檔案提交到CA以簽署憑證。如果您的組織生成自己的自簽名證書,則您可以使用
3.	CSR檔案生成自簽名證書。
步驟 4.	在Intersight中建立證書管理策略並貼上證書和私鑰對鏈。

建立配置檔案(.cnf)

使用檔案編輯器建立副檔名為.cnf的配置文件。根據您的組織詳細資訊填寫設定。

<#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

⚠ 註意:使用主體替代名稱為伺服器指定其他主機名或IP地址。不對其進行配置或將其從上傳的 證書中排除,可能會導致瀏覽器阻止對Cisco IMC介面的訪問。

生成私鑰(.key)

使用 openssl genrsa 以便生成新金鑰。

<#root>

Test-Laptop\$

openssl genrsa -out cert.key 2048

驗證名為的檔案 cert.key 通過 ls -la 指令。

<#root>

Test-Laptop\$

ls -la | grep cert.key

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

產生CSR

使用 openssl req -new 為了請求 .csr 檔案使用私鑰和 .cnf 先前建立的檔案。

<#root>

Test-Laptop\$

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

使用 ls -la 以驗證 cert.csr 已建立。

<#root>

Test-Laptop\$

ls -la | grep .csr

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

註:如果您的組織使用證書頒發機構(CA),則您可以提交此CSR,以便讓您的CA簽署證書。

生成證書檔案

生成.cer x509代碼格式的檔案。

<#root>

Test-Laptop\$

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

```
使用 ls -la 以驗證 certificate.cer 已建立。
```

<#root>

Test-Laptop\$

ls -la | grep certificate.cer

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

在Intersight中建立證書管理策略

登入您的Intersight帳戶,導航至 Infrastructure Service,按一下 Policies 頁籤,然後按一下 Create Policy.

Servers	Policies		Create Policy
Chassis			
Fabric Interconnects	* All Policies © +	G Emort 217 Home found	7 x per page 27 1 of 21 5 1
HyperFlex Clusters		E Capart 217 Items round	ha ha ha a s s s s s s s s s
Integrated Systems	Platform Type Usage		X
Configure ^	UCS Server 169 UCS Chassis 14 Used 118		
Profiles	UCS Domain 64 HyperFiex Cluster 7 • • • • • • • • • • • • • • • • • •		
Templates	Name : Platform Type Type : Usage Last Update		: 9
Policies	Port_AntGeoSam UCS Domain Port 2 🔞 31 minutes ago		

按UCS伺服器過濾並選擇 Certificate Management.

<pre> Policies Create </pre>					
Filters	Q, Search				
Platform Type	Adapter Configuration	C FC Zone	Local User	◯ SNMP	
• All	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	
Kubernetes Cluster	 Certificate Management 	Http Proxy Policy	Node OS Configuration	System QoS	
	Container Runtime	IMC Access	○ NTP	Thermal	

使用 cat 命令複製憑證的內容(certificate.cert 檔案)和金鑰檔案(cert.key 檔案)並將它們貼上到Intersight中的 證書管理策略中。

<#root>

Test-Laptop\$

cat certificate.cert

Test-Laptop\$

cat cert.key

¢.	Overview	Dark theme is now available in Intersight. To switch the theme go to the User Settings					
0	Operate Servers Chassis	^	Policies > Certificate Management > Certificate-Test Edit				
,e 	Fabric Interconnects HyperFlex Cluaters Integrated Systems Configure Profiles Policies Policies Pools	^	General Policy Details	Policy Details Add policy details This policy is applicable only for UCS Servers (FI-Attached) Image: Certificate * Private Key Private Key Priv	Enabled		
Nevi to H	Command Palette gate Intersight with Ctri-K or p elp > Command Palette	× 90	K	Cancel Back	Update		
Eá	驗證具不可建立無錯誤的笑赅						

驗證是否已建立無錯誤的策略。

Policies	Successfully created policy Certificate-TAC	×
----------	---	---

將策略新增到伺服器配置檔案

導航至 Profiles 頁籤並修改伺服器配置檔案,或者建立新的配置檔案並附加其他策略(如果需要)。 此示例修改服務配置檔案。按一下 edit 然後繼續,附加策略,並部署伺服器配置檔案。

General	Management Configuration Create or select existing Management policies that you want to associate with this profile.			
Server Assignment		Certificate Management		
Compute Configuration		IMC Access	KVM-IMM	
Management Configuration		IPMI Over LAN		
	1	Local User		
5 Storage Configuration		Serial Over LAN		
6 Network Configuration		SNMP		
		Syslog		
7 Summary		Virtual KVM	KVM_IMM	

疑難排解

如果您需要檢查憑證、CSR或私鑰中的資訊,請如上所述使用OpenSSL命令。

若要檢查CSR詳細資訊:

<#root>

Test-Laptop\$

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

若要檢查憑證詳細資訊:

<#root>

Test-Laptop\$

openssl x509 -in cert.cer -text -noout

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。