# 生成和新增安裝安全端點私有雲3.x及更高版本所 需的證書

## 目錄

簡介 必要條件 需求 採用元件 背景資訊 憑證建立 在Window伺服器上生成證書 生成證書簽名請求(CSR) 將CSR提交到CA並生成證書 匯出私鑰並轉換為PEM格式 在Linux伺服器上生成證書(已禁用嚴格SSL檢查) 生成自簽名RootCA 為每個服務生成證書 生成私鑰 產生CSR 生成證書 在Linux伺服器上生成證書(已啟用嚴格SSL檢查) 生成自簽名RootCA 為每個服務生成證書 建立擴展配置檔案並儲存(extensions.cnf) 生成私鑰 產生CSR 生成證書 將證書新增到Secure Console私有雲 驗證 疑難排解 簡介

本文檔介紹生成證書的過程,每次全新安裝Secure Console Private Cloud時必須上傳這些證書,或

## 必要條件

### 需求

本文中的資訊係根據以下軟體和硬體版本:

• Windows Server 2008

者續訂已安裝的證書服務。

- CentOS 7/8
- •安全主控台虛擬私有雲3.0.2(新版本)
- OpenSSL 1.1.1

### 採用元件

思科建議您瞭解以下主題:

- Windows Server 2008(以後)
- 安全控制檯私有雲安裝
- 公開金鑰基礎架構
- OpenSSL
- Linux CLI

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

引入安全控制檯私有雲3.X後,以下所有服務都需要主機名和證書/金鑰對:

- •管理門戶
- •身份驗證(專用雲3.X中的新功能)
- 安全主控台
- •處置伺服器
- Disposition Server 擴展協定
- •處置更新服務
- Firepower管理中心

本文探討產生和上傳所需憑證的快速方式。您可以根據組織的策略調整每個引數,包括雜湊演算法

、金鑰大小和其他引數,並且生成這些證書的機制可能與此處詳細介紹的內容不匹配。

警告:下面提到的步驟可能因您的CA伺服器配置而異。預期您選擇的CA伺服器已經調配,而 且其配置已完成。以下技術說明僅描述生成證書的示例,思科TAC不參與任何型別的證書生成 和/或CA伺服器問題故障排除過程。

## 憑證建立

### 在Window伺服器上生成證書

確保在Windows Server上安裝並配置以下角色。

- Active Directory證書服務
- 證書頒發機構
- 證書頒發機構Web註冊
- 聯機響應程式
- 證書註冊Web服務
- 證書註冊策略Web服務

- Active Directory域服務
- DNS伺服器
- •Web伺服器(IIS)
- Active Directory Certificate Services
- Active Directory Domain Services
   DNS Server
   File Services
- Web Server (IIS)

### 生成證書簽名請求(CSR)

步驟1.導航到MMC控制檯,然後為您的電腦帳戶新增「證書」管理單元,如下圖所示。

p⊣in	Vendor 🔺		Console Root	Edit Extensions
Active Directory Do Active Directory Site	Microsoft Cor Microsoft Cor		Certificates (Local Computer)	Remove
ActiveX Control	Microsoft Cor			Move Up
Authorization Manager Certificate Templates	Microsoft Cor Microsoft Cor	Add >		Move Down
Certificates Certification Authority	Microsoft Cor Microsoft Cor			
Component Services	Microsoft Cor Microsoft Cor			
Vevice Manager	Microsoft Cor			
NS	Microsoft Cor			Advanced
-				

步驟2.深入查看Certificates(Local Computer)> Personal > Certificates。

步驟3.按一下右鍵空白區域,然後選擇「所有任務」>「高級操作」>「建立自定義請求」。

All Tasks Refresh	•	Request New Certificate Import		
Export List		Advanced Operations	•	Create Custom Request
View	+			Manage Enrolment Policies
Arrange Icons Line up Icons	۲			
Help				

e	rtificate Enrollment
	rtificate Enrollment
	Before You Begin
	The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.
	Before requesting a certificate, verify the following:
	Your computer is connected to the network You have credentials that can be used to verify your right to obtain the certificate
	Learn more about digital certificates
	Next Cance

步驟5.選擇您的證書註冊策略,然後選擇**下一步**。

👝 Certificate Enrollment	_ O X		
] Certificate Enrollment			
Select Certificate Enrollment Policy			
Certificate enrolment policy enables enrolment for certificates based on predefined certificate enrolment policy may already be configured for you.	e templates. Certificate		
Configured by your administrator			
Active Directory Enrolment Policy	0		
Configured by you	Add New		
Custom Request			
Proceed without enrolment policy			
Learn more about certificate enrolment policy			
	Next Cancel		

步驟6.選擇模板作為Web Server,然後選擇Next。

ertificate Enrollment		
ertificate Enrollment		
Custom request		
Chose an option from t	the list below and configure the certificate options as required.	
Template:	Web Server	
Request format:	PKCS #10	
	C CMC	
Note: Key archival is r specified in the certific	not available for certificates based on a custom certificate request, even when this option is cate template.	
Learn more about <u>cust</u>	om request	
	Next Cancel	

步驟7.如果「Web Server」模板已正確配置且可用於註冊,則顯示「可用」狀態。選擇**Details**以展 開Properties。

Certificate Enrollment		_ 0		
Certificate Enrollment				
Certificate Information				
Click Next to use the options al and then click Next.	ready selected for this template, or click Details to customize the certificate	e request,		
Active Directory Enr	oliment Policy			
Web Server	③ STATUS: Available	Details (8)		
The following options des Key usage: Application policies: Validity period (days)	cribe the uses and validity period that apply to this type of certificate: Digital signature Key encipherment Server Authentication : 730	operties		
Learn more about <u>certificates</u>				
	Next	Cancel		

步驟8.至少要新增CN和DNS屬性。可以根據您的安全要求新增其餘屬性。

rtificate Properties	Private Key	<u> </u>
The subject of a certificate is the us enter information about the types o in a certificate.	er or computer to which the fubject name and altern	he certificate is issued. You can ative name values that can be used
Subject of certificate		
The user or computer that is receiving	ng the certificate	
Subject name:		
Type:		CN=amp-vpc.cisco.com
Common name	Add >	
Value:		
	< Remove	
Alternative name:		DAIM
Type:		amp-vpc.cisco.com
DNS 💌		
Value:		
	Add >	
	< Remove	
earn more about subject name		
	OK	Cancel Anoly

步驟9.(可選)在General頁籤下提供友好名稱。

步驟10.在Private Key頁籤上選擇,並確保在Key Options部分下啟用Make private key exportable。

Certificate Properties	×
🔥 Subject   General   Extensions   Private Key	
Cryptographic Service Provider	۲
Key options         Set the key length and export options for the private key.         Key size:       2048         Make private key exportable         Allow private key to be archived         Strong private key protection	(1)
Key type	۲
Key permissions	۲
Learn more about <u>private key</u>	
OK Cancel	Apply

步驟11.最後,在**OK**中選擇。您必須進入「Certificate Enrollment」(證書註冊)對話方塊,從中可 以選擇**Next**。

步驟12.瀏覽到儲存提交到CA伺服器進行簽名的.req檔案的位置。

### 將CSR提交到CA並生成證書

步驟1.按如下所示導航到MS AD Certificate Services網頁,然後選擇Request a Certificate。

Microsoft Active Directory Certificate Services -- bgl-amp-AD-CA

## Welcome

Use this Web site to request a certificate for your Web brov request, perform other security tasks.

You can also use this Web site to download a certificate au

For more information about Active Directory Certificate Ser

## Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

步驟2.在「advanced certificate request」連結上進行選擇。

Microsoft Active Directory Certificate Services -- bgl-amp-AD-CA

## **Request a Certificate**

Select the certificate type: User Certificate

Or, submit an advanced certificate request.

步驟3.選擇Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file or submit a renewal request by using a base-64-encoded PKCS #7 file。

步驟4.通過記事本開啟先前儲存的.req檔案(CSR)的內容。複製內容並貼上到此處。確保將證書模板 選為Web Server



#### Submit a Certificate Request or Renewal Request

REQ1 · Notepad

Saved Request			
Base 64-encoded cettificate request (CMC er PNCS #10 er PNCS #7):	BEGIN NEW NIIDubCCAgACAg nd OwgeEIMAOCO VJeBNC21F#ENA VWEMC24FrJW NeWCaaFelyV90C 4	CERTIFICATE REQ IN/TEINCEGALUERA gid In DOGENACIENA DUCLI/OC/JADEA/Hy CVV/c00981.0W/21100 yej Ozyp709588230	VEST * veIslyIS1) IBDv0vegEE COMMINUTV 1550057240 schyfnRoeT *
Certificate Temp	date:		
	Web Sener	-	
Additional Attrib	utes:		
Attributes		2	-
			Robert L

Hold - Molecular
 The Edit Format View Help
 The Control of the Provided State Assessment Pyrt 51 (b) 3 (b) 1 (b) 1

#### 步驟5.最後,選擇Submit。

步驟6.此時,您必須能夠Download憑證,如下圖所示。

Certificate Issued
The certificate you requested was issued to you.
DER encoded or      Dase 64 encoded      Download certificate     Download certificate chain

#### 匯出私鑰並轉換為PEM格式

步驟1.通過開啟.cer檔案並選擇安裝證書,將證書安裝到您的證書儲存區。

步驟2.導航到之前選擇的MMC管理單元。

步驟3.導航到安裝證書的儲存。

步驟4.按一下右鍵正確的證書,選擇**所有任務>匯出**。



步驟5.在「Certificate Export Wizard(證書匯出嚮導)」中,確認匯出私鑰,如下圖所示。

ertificate Export Wizard	×			
Export Private Key				
You can choose to export the private key with the certificate.				
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.				
Do you want to export the private key with the certificate?				
Yes, export the private key				
C No, do not export the private key				
Learn more about exporting private keys				
< Back Next > Can	cel			

步驟6.輸入密碼,然後選擇Next將私鑰儲存到磁碟上。

步驟7.這會以.PFX格式儲存私鑰,但是,需要將其轉換為.PEM格式才能將其用於安全終結點私有雲。

步驟8.安裝OpenSSL庫。

步驟9.開啟命令提示符視窗,並轉到安裝OpenSSL的目錄。

步驟10.運行以下命令提取私鑰並將其儲存到新檔案:(如果PFX檔案與儲存OpenSSL庫的路徑不同,則必須指定確切路徑以及檔名)

openssl pkcs12 -in yourpfxfile.pfx -nocerts -out privatekey.pem -nodes 步驟11.現在,運行以下命令來提取公共證書並將其儲存到新檔案:

openssl pkcs12 -in yourpfxfile.pfx -nokeys -out publiccert.pem -nodes 在Linux伺服器上生成證書(已禁用嚴格SSL檢查)

注意:嚴格TLS檢查驗證證書是否滿足Apple的TLS要求。如需詳細資訊,請參閱<u>管理指南</u>。

確保您嘗試生成所需證書的Linux伺服器安裝了OpenSSL 1.1.1庫。驗證此操作以及下面列出的過程 是否可能與您正在運行的Linux發行版不同。此部分已記錄在案,在CentOS 8.4伺服器上完成。

### 生成自簽名RootCA

#### 步驟1.生成根CA證書的私鑰。

openssl genrsa -out 步驟2.生成CA證書。

```
openssl req \
-subj '/CN=
-addext "extendedKeyUsage = serverAuth, clientAuth" \
-outform pem -out
-key
-days "1000"
```

#### 為每個服務生成證書

根據DNS名稱條目為身份驗證、控制檯、處置、處置擴展、更新伺服器、Firepower管理中心 (FMC)服務建立證書。您需要為每個服務(身份驗證、控制檯等)重複以下證書生成過程。

	Certificate (PEM .crt)		<pre> Qe Key (PEM .key) </pre>
0	Certificate file has been uploaded.	٥	Key file has been uploaded.
0	Certificate is in a readable format.	٥	Key contains a supported key type.
0	Certificate start and end dates are valid.	٥	Key contains public key material.
0	Certificate contains a subject.	٥	Key contains private key material.
0	Certificate contains a common name.	٥	Key contains a public key matching the uploaded certificate
0	Certificate contains a public key matching the uploaded key.		+ Choose Ke
0	Certificate matches hostname.		
0	Certificate is signed by a trusted root authority.		
	+ Choose Cartificate		

#### 生成私鑰

openssl genrsa -out

將<YourServiceName.key>替換為要建立為Auth-Cert.key的新金鑰檔名

#### 產生CSR

openssl req -new \
-subj '/CN=
-key

更換 <YourServiceName.key>使用當前(或新)證書KEY檔案,例如Auth-Cert.key

將<YourServiceName.csr>替換為要建立的CSR檔名,例如Auth-Cert.crt

### 生成證書

openss1 x509 -req \ -in -CAkey -days 397 -sha256 將<YourServiceName.csr>替換為實際(或新)的憑證CSR,例如Auth-Cert.csr

將<YourRootCAName.pem>替換為實際(或新)的PEM檔名RootCAName.pem

將<YourServiceName.key>替換為當前(或新)的證書KEY檔案,如Auth-Cert.key

將<YourServiceName.crt>替換為要建立的檔名,如Auth-Cert.crt

## 在Linux伺服器上生成證書(已啟用嚴格SSL檢查)

**注意**:嚴格TLS檢查驗證證書是否滿足Apple的TLS要求。如需詳細資訊,請參閱<u>管理指南</u>。

### 生成自簽名RootCA

步驟1.生成根CA證書的私鑰。

openssl genrsa -out 步驟2.生成CA證書。

openssl req \ -subj '/CN= -outform pem -out -key -days "1000"

### 為每個服務生成證書

根據DNS名稱條目為身份驗證、控制檯、處置、處置擴展、更新伺服器、Firepower管理中心 (FMC)服務建立證書。您需要為每個服務(身份驗證、控制檯等)重複以下證書生成過程。

-subj ' / ™= -out 更換 <YourServiceName.key>使用當前(或新)證書金鑰,例如Auth-Cert.key

#### 產生CSR

-kev

openssl req -new \

openssl genrsa -out 將<YourServiceName.key>替換為要建立為Auth-Cert.key的新金鑰檔名

#### 生成私鑰

```
[v3_ca]
basicConstraints = CA:FALSE
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = critical, serverAuth, clientAuth
```

### 建立擴展配置檔案並儲存(extensions.cnf)

```
Replace Certificate
AMP for Endpoints Console Certificate
                                                                                    Disable Strict TLS Check
                                                                                                                   Undo

    Certificate (PEM .crt)

                                                                                                  Q. Kov (DEM
                                                                                                                 key)
         Certificate file has been uploaded.
                                                                                 Key file has been uploaded.
   0
                                                                           0
                                                                                  Key contains a supported key type.
         Certificate is in a readable format.
   0
                                                                           0
                                                                           0
         Certificate start and end dates are valid.
                                                                                 Key contains public key material.
   0
                                                                                 Key contains private key material.
         Certificate contains a subject.
   0
                                                                           0
         Certificate contains a common name.
                                                                                 Key contains a public key matching the uploaded certificate.
   0
                                                                           0
         Certificate contains a public key matching the uploaded key.
   0
                                                                           Ŀ
                                                                                                                             + Choose Key
         Certificate matches hostname.
   0
         Certificate is signed by a trusted root authority.
   0
         Certificate issued after 07/01/2019 must have a validity period
   0
         of 825 days or less.
         Certificate issued after 09/01/2020 must have a validity period
  0
         of 398 days or less.
         Certificate does not use sha-1 signature algorithm.
   0
         Certificate using RSA keys must use a key size of 2048 or
   0
         more.
         Certificate must specify server certificate in Extended Key
   0
         Usage extension.
                                               + Choose Certificate
```

#### 生成證書

openssl x509 -req -in -CA -CAcreateserial -out -extensions v3\_ca -extfile extensions.cnf \ -days 397 -sha256 將<YourServiceName.csr>替換為當前(或新)的證書CSR,例如Auth-Cert.csr 將<YourRootCAName.pem>替換為當前(或新)的PEM檔名RootCAName.pem

將<YourServiceName.key>替換為當前(或新)的證書KEY檔案,如Auth-Cert.key

將<YourServiceName.crt>替換為要建立的檔名,如Auth-Cert.crt

## 將證書新增到安全控制檯私有雲

步驟1.從上述任何方法生成證書後,上傳每個服務的相應證書。如果生成正確,則會啟用所有複選 標籤,如下圖所示。



## 驗證

目前沒有適用於此組態的驗證程序。

## 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

#### 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)。