配置Finesse和CTI伺服器之間的安全通訊

目錄

簡介 必要條件 需求 採用元件 背景資訊 設定 CCE CTI伺服器安全 Finesse安全配置 生成代理PG證書(CTI伺服器) 獲取CA簽名的CSR證書 匯入CCE PG的CA簽名證書 生成Finesse證書 由CA簽署Finesse證書 匯入Finesse應用程式和根簽名的證書 驗證 疑難排解

簡介

本檔案介紹如何在Cisco Contact Center Enterprise(CCE)解決方案中的Cisco Finesse和Computer Telephony Integration(CTI)伺服器之間實作憑證授權單位(CA)簽署的憑證。

必要條件

需求

思科建議您瞭解以下主題:

- CCE版本12.0(1)
- Finesse版本12.0(1)
- CTI伺服器

採用元件

本檔案中的資訊是根據以下軟體版本:

- 套裝CCE(PCCE)12.0(1)
- Finesse 12.0(1)

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CCE版本11.5中,思科開始支援傳輸層安全(TLS)版本1.2,該版本允許通過TLS 1.2安全地傳輸會 話初始協定(SIP)和即時傳輸協定(RTP)消息。從CCE 12.0開始,作為保護移動資料的一部分,思科 開始在大部分聯絡中心呼叫流上支援TLS 1.2:入站和出站語音、多通道和外部資料庫。本文的重點 是入站語音,特別是Finesse和CTI伺服器之間的通訊。

CTI伺服器支援以下連線模式:

- **僅安全連線**:允許在CTI伺服器和CTI客戶端(Finesse、撥號器、CTIOS和ctitest)之間進行安全 連線。
- **安全連線和非安全連線(混合模式)**:允許在CTI伺服器和CTI客戶端之間進行安全連線和非安 全連線。這是預設連線模式。將先前版本升級到CCE 12.0(1)時將配置此模式。

附註:不支援僅非安全模式。

設定

CCE CTI伺服器安全

步驟1.在PCCE管理工作站(AW)上,開啟**Unified CCE Tools**資料夾,然後按兩下**Peripheral** Gateway Setup。



步驟2.選擇CG3A,然後按一下Edit。

Cisco Unified ICM/Contact Cer	nter Enterprise Components Setup
ICM Instances Add Edit Delete To set up Administration Data Server (Dir Interface Controller (NIC), WebView or N Web Setup tool. To set up Administration Client (Client AW and Setup tool. The Instance cc cannot be deleted becc Web Setup or Administration Client Setup to remove those components before deleted Setup.	Instance Components Add PG1A PG2A PG3A PG3A RoutesA Delete Delete V), use the Administration Client Installer suse it has components set up by the p tool. You must use the applicable tool sting the instance in Peripheral Gateway
	Help Exit Setup

步驟3.在CTI伺服器屬性上,按一下**下一步**。有關設定停止**CG**3A服務**的問題,**請選擇**Yes**。

步驟4.在CTI伺服器元件屬性上,選擇啟用僅安全模式。請注意安全連線埠(46030),因為在下一個 練習中,您必須在Finesse中配置相同的埠。按「Next」(下一步)。

CTI Server Component Properties
CTI Server configuration
Secured Connection Port 46030
Non-Secured Connection Port 42027
Agent Login Required for Client Events
Help < Back Next> Cancel

附註:預設安全通訊為42030,但本文檔使用的實驗為40630。埠號是包括ICM系統ID的公式 的一部分。當系統id為1(CG1a)時,預設埠號通常為42030。由於實驗中的系統id為 3(CG3a),因此預設埠號為46030。

步驟5.在CTI Network Interface Properties上,按一下「Next」。檢查Setup Information,然後按一 下Next。

Unified ICM/CCE PGSetup: cc-CG3A	×
Check Setup Information	Z
Setup has enough information to begin the configuration operation. If you want to review or change and of the settings, click Back. If satisfied, click Next to begin configuring the CTI Gateway.	
Current Settings:	
Setup Type: CTI Gateway, side A	~
Target Directory: C:ljicm	=
Configuration: PG node is pocealin1p CTI Gateway is simplexed DMP address is 3	~
<	>
InstallShield	
< Back Next :	Cancel

步驟6.按一下Finish,如下圖所示。

Unifie	ed ICM/CCE PGSetup: cc-CG3A	
	Setup Complete PGSetup is complete. You may start the Unified ICM/CC Node Manager service now by checking the box below. Yes, start the Unified ICM/CC Node Manager Click Finish to Complete Setup.	
< Back Finish Cancel		

步驟7.按一下Exit Setup,並等待設定視窗關閉為止,如下圖所示。

ICM Instances	Inc	tance Components	
ee	Add	W 1634	Add
	5 D P	oggerA G1A	
	Edit	G2A	Edit
	Delete	louterA	Delete
To set up Administration Interface Controller (NIC	Data Server (Distribut), WebView or Networ	or AW), Router, Logge k Gateway componen/	r, Network s, use the
To set up Administration Interface Controller (NIC Web Setup tool. To set up Administration and Setup tool.	Data Server (Distribut), WebView or Networ Client (Client AW), use	or AW], Router, Logge k Gateway component the Administration Cliv	r, Network is, use the ent Installer
To set up Administration Interface Controller (NIC Web Setup tool. To set up Administration and Setup tool. The Instance cc canno Web Setup or Administr to remove those compo	Data Server (Distribut), WebView or Network Client (Client AW), use t be deleted because it ation Client Setup tool. nents before deleting ti	or AW], Router, Logge k Gateway component the Administration Cli has components set o You must use the app he instance in Peripher	r, Network is, use the ent Installer ap by the licable tool al Gateway
To set up Administration Interface Controller (NIC Web Setup tool. To set up Administration and Setup tool. The Instance cc canno Web Setup or Administr to remove those compo Setup.	Data Server (Distribut), WebView or Network Client (Client AW), use t be deleted because it ation Client Setup tool, nents before deleting ti	or AW], Router, Logge k Gateway component the Administration Cli has components set of You must use the app he instance in Peripher	r, Network is, use the ent Installer ap by the licable tool al Gateway
To set up Administration Interface Controller (NIC Web Setup tool. To set up Administration and Setup tool. The Instance cc canno Web Setup or Administr to remove those compo Setup.	Data Server (Distribut), WebView or Networ Client (Client AW), use t be deleted because it ation Client Setup tool. nents before deleting ti	or AW), Router, Logge k Gateway component the Administration Clin has components set of You must use the app he instance in Peripher	r, Network s, use the ent Installer ap by the licable tool al Gateway

步驟8.在PCCEAlin1案頭上,按兩下Unified CCE service Control。

步驟9.選擇Cisco ICM cc CG3A,然後按一下Start。

Finesse安全配置

步驟1.開啟Web瀏覽器並導航至Finesse Administration。

步驟2.向下滾動至Contact Center Enterprise CTI Server Settings部分,如下圖所示。

Note: Any changes made to Contact Center Enterpris	the settings on this gadget re ie CTI Server Settings	quire a restart of Cisco Finesse Torncat to t	ake effect.
A Side Host/IP Address*	10.10.10.10	B Side Host/IP Address	
A Side Port*	42027	B Side Port	
Peripheral ID*	5000		

步驟3.更改在上一個練習中在CG3A上配置的安全通訊埠的A側埠:46030。選中**Enable SSL**encryption,然後點選Save。

Contact Center Ent	erprise CTI Server S	iettings	
Note: Any changes made to Contact Center Enterpris	o the settings on this gadget ise CTI Server Settings	require a restart of Cisco Finesse Torncat to	take effect.
A Side Host/IP Address*	10.10.10.10	B Side Host/IP Address	
A Side Port*	46030	B Side Port	
Peripheral ID*	5000		
Enable SSL encryption	rt		

附註: 為了測試連線,您需要先重新啟動Finesse Tomcat服務或重新啟動Finesse伺服器。

步驟4.從Finesse管理頁面註銷。

步驟5.使用Finesse開啟SSH會話。

步驟6.在FINESSEA SSH會話上,執行命令:

utils系統重新啟動

當系統詢問您是否要重新啟動系統時,輸入yes。

```
<sup>A</sup> Using username "administrator".
Command Line Interface is starting up, please wait ...
Welcome to the Platform Command Line Interface
VMware Installation:
2 vCPU: Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz
Disk 1: 146GB, Partitions aligned
8192 Mbytes RAM
admin:utils system restart
Do you really want to restart ?
Enter (yes/no)? yes
Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
```

生成代理PG證書(CTI伺服器)

CiscoCertUtils是在CCE版本12上發佈的新工具。您可以使用此工具管理入站語音的所有CCE證書 。在本文中,您使用這些CiscoCertUtils來產生外圍閘道(PG)憑證簽署請求(CSR)。 步驟1。執行此命令以產生CSR憑證:CiscocertUtil /generateCSR

C:\Users\Administrator.CC> C:\Users\Administrator.CC>CiscocertUtil /generateCSR Key already exists at C:\icm\ssl\keys\host.key. It will be used to generate the CSR. SSL config path = C:\icm\ssl\cfg\openssl.cfg SYSTEM command is C:\icm\ssl\keys\host.exe req =new =key C:\icm\ssl\keys\host. key =out C:\icm\ssl\certs\host.csr 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.

提供所需的資訊,例如:

國家/地區名稱:美國

省或州名稱:MA

地區名稱:BXB

組織名稱: 思科

組織單位:CX

公用名: PCCEAllin1.cc.lab

電子郵件:jdoe@cc.lab

質詢密碼:火車1ng!

可選的公司名稱:思科

主機證書和金鑰儲存在C:\icm\ssl\certs和C:\icm\ssl\keys中。

步驟2.導覽至C:\icm\ssl\certs資料夾,並確保已產生host.csr檔案。

獲取CSR證書 由CA簽署

產生CSR憑證後,需要由第三方CA簽署。在本練習中,安裝在域控制器中的Microsoft CA用作第三方CA。

使用Microsoft CA時,請確保CA使用的證書模板包括客戶端和伺服器身份驗證,如圖所示。

Properties of New Template	ons	
Subject Name Server Issuance Requirements Compatibility General Request Handling Cryptography Key Attestation Superseded Templates Extensions Security To modify an extension, select it, and then click Edit. Extensions included in this template:	tificate Templates More Actions b Server More Actions Edit Application P	(DC.cc.lab)
Application Policies	An application policy defi	Add Application Policy X
Certificate Template Information	Application pglicies:	An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template. Application policies:
Description of Application Policies:	Add	Artestation identity Key Centricate Centricate Request Agent Citent Authentication Code Signing CTL Usage Digital Rights Directory Service Email Replication Disallowed List Document Encryption Document Signing Domain Name System (DNS) Server Trust Dynamic Code Generator New OK Cancel

步驟1.開啟Web瀏覽器並導航至CA。

步驟2.在Microsoft Active Directory證書服務上,選擇請求證書。

_ O X
🗲 💿 🖉 https://dc.cc.lab/centinv/en-us/ 🛛 🖓 🖷 C 🧭 Microsoft Active Directory × 👘 🏠 🔅
Microsoft Active Directory Certificate Services - cc-DC-CA Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services</u> Documentation.
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

步驟3.選擇advanced certificate request選項。

Micr	rosoft Activ	e Directory Ce	ertifical × +				
\leftrightarrow	С°Ш		🛈 🔒 https://dc.	c.lab/certsrv/en	-us/certr	qus.asp	_
CUCM	🛅 CUIC	🛅 Finesse	🛅 Remote Expert Mobile	🛅 MediaSense	CVP	CCE	Ē
Microsoft Request	Active Dire	ectory Certifi icate	cate Services cc-DC-0	CA			
Select the	e certific Certificat	ate type: e					_

步驟4.在「advanced certificate request」上,複製並貼上「Saved Request」框中的PG代理 CSR證書的內容。

步驟5.選擇具有客戶**端和服**務器身份驗證的**Web** Server模板。在實驗中,CC Web Server模板是使 用客戶端和伺服器身份驗證建立的。

To submit a sa	ved request to the CA, part	Copy and paste the	contents
Saved Request		or the expected CS	ik nie
Base-64-encoded entificate request CMC or %CCS #10 or %CCS #7):	3LhnlD3GsLbIYivb7lbshW gWL/H3DRlnRpJtLKfnLGgX +L3E0yNQ+W9/SJojYzBGnH J75nKDoyAh7C+F0u9tmg261 rArT900dxJem END CERTIFICATE RI <	fqH1509jMcZ3uZrciC SkUAZqin/S6HjuGb4h k38yo1P/I7UsueE3OR DZaOZ3k9Wo5QzUTPmd EQUESTsna	*
ertificate Temp	late:		_
	CC Web Server	<u> </u>	
dditional Attrib	utes:		_
		а	
Attributes:			

步驟6.按一下Submit。

步驟7.選擇Base 64 encoded,然後按一下Download Certificate,如下圖所示。

Microsoft Active Directory Certificate Services -- cc-DC-CA

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

b	٥	~	1		
ł	¢	è	4		1
-	-	-	20	-	

Download certificate Download certificate chain

步驟8.儲存檔案,然後按一下OK。檔案儲存在Downloads資料夾中。

步驟9.將檔案重新命名為host.cer(可選)。

步驟10。您還需要生成根證書。返回CA證書頁面,然後選擇下載CA證書、證書鏈或CRL。您只需 執行一次此步驟,因為所有伺服器(PG代理和Finesse)的根證書都相同。



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

步驟11.按一下Base 64,然後選擇Download CA certificate。

Microsoft Active Directory Certificate Senices cc-DC-CA
Download a CA Certificate, Certificate Chain, or CRL
To trust certificates issued from this certification authority,
To download a CA certificate, certificate chain, or CRL, se
CA certificate:
Current (cc-DC-CA)
Encoding method:
ODER ⊛Base 64
Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

步驟12.按一下Save File,然後選擇OK。檔案將儲存在預設位置Downloads。

匯入CCE PG的CA簽名證書

步驟1。在PG Agent上,導航至C:\icm\ssl\certs,然後在此處貼上根和PG Agent簽名的檔案。

步驟2.將c:\icm\ssl\certs上的host.pem證書重新命名為selfhost.pem。

步驟3.將c:\icm\ssl\certs資料夾上的host.cer重新命名為host.pem。

步驟4.安裝根證書。在命令提示符下,發出以下命令:CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer



步驟5. 安裝運行相同命令的應用程式簽名證書: CiscoCertUtil /install C:\icm\ssl\certs\host.pem



步驟6.循環PG。開啟Unified CCE Service Control,然後循環Cisco ICM Agent PG。

生成Finesse證書

0

步驟1.開啟Web瀏覽器並導航至Finesse OS Admin。

步驟2.使用作業系統管理員憑證登入,然後導覽至Security > Certificate Management,如下圖所示



步驟3.按一下Generate CSR,如下圖所示。



步驟4.在Generate Certificate Signing Request上,使用預設值,然後點選Generate。

Generate Certificate Signing Request					
💽 Generate 🖳 Close					
Gular					
Warning: Canaratio	a a new CEB for a specific partificate type will suprovide the existing CEB for that type				
	g a new cak for a specific certainate type will overwrite one existing cak for this type				
Generate Certificate 5	Signing Request				
Certificate Purpose**	tomcat v				
Distribution*	FINESSEA.cc.lab v				
Common Name*	FINESSEA.cc.lab				
Subject Alternate Nam	mes (SANs)				
Parent Domain	cc.iab				
Key Type**	RSA				
Key Length	2048 v				
Hash Algorithm*	SH4256 V				
Generate Close					
(i) *- indicates require	ed item.				
When the Certifi	When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Eliptic Curve (EC). Otherwise, it				
is RSA.					

步驟5.關閉Generate Certificate Signing Request視窗並選擇Download CSR。

Show *	Settings *	Security *	Software Upgrades *	Services *	Help *		
Certifica	ite List						
Gen	erate Self-sign	ed 🐴 Up	load Certificate/Certificate	chain 💽	Generate CSR	Download CSR	

步驟6.在「憑證用途」上,選擇tomcat,然後按一下Download CSR。

Download Certificate Signing Request
Download CSR 🕎 Close
Status
Certificate names not listed below do not have a corresponding CSR
Certificate Signing Request
Download CSR Close
 indicates required item.
C >

步驟7.選擇Save File,然後按一下OK,如下圖所示。

Opening tomcat.csr		×
You have chosen to tomcat.csr which is: csr	open: File	
from: https://	/finessea.cc.lab:8443	
O Open with	Browse	
Save File Do this autor	natically for files like this from now on.	
	OK Cancel	

步驟8.關閉Download Certificate Signing Request視窗。證書儲存在預設位置(此電腦>下載)。

步驟9.開啟Windows資源管理器並導航到該資料夾。按一下右鍵此證書並將其重新命名 :finessetomcat.csr

由CA簽署Finesse證書

在本節中,使用上一步中使用的Microsoft CA作為第三方CA。

附註: 確保CA使用的證書模板包括客戶端和伺服器身份驗證。

步驟1.開啟Web瀏覽器並導航至CA。

步驟2.在Microsoft Active Directory證書服務上,選擇請求證書。

_ O X
🗲 💿 🖉 https://dc.ec.lab/centinv/en-us/ 🔎 = 🔒 🖉 Microsoft Active Directory ×
Microsoft Active Directory Certificate Services - cc-DC-CA Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Active Directory Certificate Services, see <u>Active Directory Certificate Services</u> Documentation.
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

步驟3.選擇advanced certificate request選項,如下圖所示。

Micr	osoft Activ	e Directory Ce	ertifica × +				
\leftrightarrow \rightarrow	C'û		🛈 윩 https://dc.	c.lab/certsrv/en	-us/certr	qus.asp	_
🗎 СИСМ	🛅 CUIC	🛅 Finesse	🛅 Remote Expert Mobile	🛅 MediaSense	CVP	🛅 CCE	
Microsoft	Active Dir	ectory Certifi	cate Services cc-DC-0	CA			
Request	a Certif	icate					_
Select the User C	e certific Certificat	ate type:					
Or, subm	it an <mark>adv</mark>	anced cer	rtificate request.				

步驟4.在**進階憑證請求**上,複製並貼上**Saved Request**方塊中Finesse CSR憑證的內容。

步驟5.選擇具有客戶端和伺服器身份驗證的Web伺服器模板。在本實驗中,CC Web Server模板是 使用客戶端和伺服器身份驗證建立的。

Microsoft Active	Microsoft Active Directory Certificate Services - cc-DC-CA					
Submit a Certificate Request or Renewal Request						
To submit a say Saved Request	ved request to the CA, part to the CA, part to the CA, part to the the total to the	Copy and paste th of the expected C	e contents ⁹ K(SR file			
Saved Request:			_			
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	SLhnlD3GsLbIYivb7IbshW gWL/H3DR1nRpJtLKfnLGgX +L3E0yNQ+W9/SJojYzBGnH J75nKDoyAh7C+F0u9tmg261 rArT9OOdxJem END CERTIFICATE RI <	fqH1509jMcZ3uZrciC SkUAZqin/56HjuGb4h k38yo1P/I7UsueE3OR DZaOZ3k9Wo5QzUTPmd EQUESTsna	< × ×			
Certificate Templ	late:					
	CC Web Server	~	_			
Additional Attribu	utes:		_			
Attributes:		a.				
		Submit >	_			

步驟6.按一下Submit。

步驟7.選擇Base 64 encoded,然後按一下Download certificate,如下圖所示。

Microsoft Active Directory Certificate Services -- cc-DC-CA

Certificate Issued

The certificate you requested was issued to you.

ODER encoded or
Base 64 encoded

 Download certificate

 Download certificate chain

步驟8.儲存檔案,然後按一下OK。檔案儲存在Downloads資料夾中。

步驟9.將檔案重新命名為finesse.cer。

匯入Finesse應用程式和根簽名的證書

步驟1。在Web程式上,開啟Finesse OS Admin頁面並導航至Security> Certificate Management。

步驟2.按一下Upload Certificate/Certificate chain按鈕,如下圖所示。

	-
Generate Self-signed Upload Certificate/Certificate chain	Generate CSR
Certificate List	
Find Certificate List where Certificate 💌 begins with	V

步驟3.在快顯視窗中選擇tomcat-trust for Certificate Purpose。

步驟4.按一下Browse...按鈕,選擇要匯入的根證書檔案。然後按一下Open按鈕。

步驟5。在說明中寫入類似tomcatrootcert的內容,然後按一下Upload按鈕,如下圖所示。

Upload Certificate/Certific	ate chain
Dipload 🖳 Close	
Status Warning: Uploading a clo	ster-wide certificate will distribute it to all servers in this cluster
Upload Certificate/Certifi	cate chain
Certificate Purpose	tomcat-trust
Upload File	Browse rootAll.cer
Upload Close	
(i) *- indicates required ite	m.
£	

步驟6.等到您看到Success:Certificate Uploaded消息以關閉視窗。

系統將要求您重新啟動系統,但首先繼續上傳Finesse應用程式簽名的證書,然後您可以重新啟動系 統。

0 🕰	https://finessea.cc.lab:	8443/cmplatform/certificateUpload.do		${igsidential}$	☆	≡
Upload	Certificate/Certificat	e chain				
De Con	oad 🔄 Close					
Status (i) s (i) R	s uccess: Certificate Uplos estart the node(s) using	ded the CLI command, "utils system restart".				
Uploa	d Certificate/Certifica	ite chain				_
Certifi	cate Purpose*	tomcat-trust	~			
Upload	f File	Browse No file selected.				
Uplo	ad Close	 、				_
		na				>

步驟7.按一下Upload Certificate/Certificate chain按鈕上的更多時間以匯入Finesse應用程式證書。

Certificate List	
Generate Self-signed	Upload Certificate/Certificate chain
Contificate List	
Certificate List	
Find Certificate List whe	re Certificate Degins with
	la ser a
Generate Self-signed	Upload Certificate/Certificate chain Generate CSR

步驟8.在快顯視窗中選擇tomcat for Certificate Purpose。

步驟9.按一下Browse...按鈕,然後選擇Finesse CA簽名檔案finesse.cer。然後按一下Open按鈕。

步驟10.按一下Upload按鈕。

and The sure			
Upload Close			
tatus			
1.45 1.45 19			
D			
Warning: Uploading a cl	uster-wide certificate will distribute it to all servers	in this cluster	
Warning: Uploading a cl	uster-wide certificate will distribute it to all servers	in this cluster	
Warning: Uploading a cli Upload Certificate/Certific Certificate Purpose*	uster-wide certificate will distribute it to all servers cate chain	in this cluster	
Warning: Uploading a clu Upload Certificate/Certific Certificate Purpose* Description(friendly name)	uster-wide certificate will distribute it to all servers cate chain tomcat Self-signed certificate	in this cluster	

步驟11.等到您看到Success:證書上傳消息。

再次請求重新啟動系統。關閉視窗並繼續重新啟動系統。

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。