CUCM第三方CA簽名LSC生成和匯入配置示例

目錄

簡介 必要條件 需求 採用元件 設定 上傳CA根證書 將證書頒發的離線CA設定為端點 為電話生成證書簽名請求(CSR) 將產生的CSR從CUCM獲取到FTP(或TFTP)伺服器 獲取電話證書 將.cer轉換為.der格式 將證書(.der)壓縮為.tgz格式 將.tgz檔案傳輸到SFTP伺服器 將.tgz檔案匯入CUCM伺服器 使用Microsoft Windows 2003證書頒發機構簽署CSR 從CA取得根憑證 驗證 疑難排解

簡介

憑證授權代理功能(CAPF)本地有效憑證(LSC)是本地簽署的。但是,您可能要求電話使用第三方證 書頒發機構(CA)簽名的LSC。本文描述了幫助您實現此目標的過程。

必要條件

需求

思科建議您瞭解Cisco Unified Communication Manager(CUCM)。

採用元件

本檔案中的資訊是根據CUCM版本10.5(2);但是此功能在10.0版及更新版本中有效。

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。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

設定

以下是此程式涉及的步驟,每個步驟在各自的章節中詳述:

- 1. 上傳CA根證書
- 2. <u>將證書頒發的離線CA設定為端點</u>
- 3. <u>為電話生成證書簽名請求(CSR)</u>
- 4. <u>將產生的CSR從Cisco Unified Communications Manager(CUCM)獲取到FTP伺服器</u>
- 5. 從CA獲取電話證書
- 6. <u>將.cer轉換為.der格式</u>
- 7. <u>將證書(.der)壓縮為.tgz格式</u>
- 8. <u>將.tgz檔案傳輸到Secure Shell FTP(SFTP)伺服器</u>
- 9. <u>將.tgz檔案匯入CUCM伺服器</u>
- 10. 使用Microsoft Windows 2003證書頒發機構簽署CSR
- 11. <u>從CA取得根憑證</u>

上傳CA根證書

- 1. 登入到思科統一作業系統(OS)管理Web GUI。
- 2. 導覽至Security Certificate Management。
- 3. 按一下「Upload Certificate/Certificate chain」。
- 4. 在Certificate Purpose下選擇CallManager-trust。
- 5. 瀏覽到CA的根憑證,然後按一下Upload。

Cisco U For Cisco U	nified Operating System Administration
Show - Settings - Se	curity 🕶 Software Upgrades 👻 Services 👻 Help 👻
🕹 Upload Certificate/Cert	ficate chain - Mozilla Firefox
https://10.106.122.173	/cmplatform/certificateUpload.do
Upload Certificate/C	ertificate chain
Upload Close	
Status Warning: Uploadi	ng a cluster-wide certificate will distribute it to all servers in this cluster
Upload Certificate/	Certificate chain
Description(friendly pa	CallManager-trust
Upload File	Browse_ AMEER-CA.cer
Upload Close	

將證書頒發的離線CA設定為端點

- 1. 登入到CUCM管理Web GUI。
- 2. 導覽至System > Service Parameter。
- 3. 選擇CUCM Server並為服務選擇Cisco Certificate Authority Proxy Function。
- 4. 選擇**離線CA**以向終端頒發證書。

Cisco Unified CM Administration	
System Call Routing Media Resources Advanced Features	Device 👻 Application 👻 User Mana <u>c</u>
Service Parameter Configuration	
Save 🧬 Set to Default	
Status	
i Status: Ready	
Select Server and Service	
Server* 10.106.122.173CUCM Voice/Video (Active)	▼
Service* Cisco Certificate Authority Proxy Function (Active)	-
All parameters apply only to the current server except parameters t	hat are in the cluster-wide group(s
Cisco Certificate Authority Proxy Function (Active) Parameter	ers on server 10.106.122.173
Parameter Name	Parameter Value
Certificate Issuer to Endpoint *	Offline CA
Duration Of Certificate Validity	5
Key Size	1024
Maximum Allowable Time For Key Generation *	30
Maximum Allowable Attempts for Key Generation *	3

為電話生成證書簽名請求(CSR)

- 1. 登入到CUCM管理Web GUI。
- 2. 導航到Device Phones。
- 3. 選擇其LSC必須由外部CA簽署的電話。
- 4. 將裝置安全配置檔案更改為安全配置檔案(如果不存在,請在安全電話安全配置檔案上新增一個系統)。
- 5. 在電話配置頁面的CAPF部分下,為認證操作選擇**安裝/升級**。對其LSC必須由外部CA簽名的 所有電話完成此步驟。對於證書操作狀態,您應該會看到**Operation Pending**。

Protocol Specific Information -		
Packet Capture Mode*	None	•
Packet Capture Duration	0	
BLF Presence Group*	Standard Presence group	•
Device Security Profile*	Cisco 7962 - Standard SCCP - Secure Profile	-
SUBSCRIBE Calling Search Space	< None >	+
Unattended Port		
Require DTMF Reception		
RFC2833 Disabled		

Certification Authority Proxy Function (CAPF) Information-

Authentication Mode*	By Nul	l Strin	g			•
Authentication String						
Generate String						
Key Size (Bits)*	2048					•
Operation Completes By	2015	1	24	12	(YYYY:MM:DD:HH)	

電話安全配置檔案(7962型號)。

	Phone Security Profi	le Configuration		
	Save 🗶 Delete	🗋 Copy 🎦 Reset 🧷 Apply Config 🕂 Add New		
	Status			
	i Status: Ready			
	-Phone Security Prof	ile Information		
	Product Type: Device Protocol:	Cisco 7962 SCCP		
	Name*	Cisco 7962 - Standard SCCP - Secure Profile		
	Description	Cisco 7962 - Standard SCCP - Secure Profile		
	Device Security Mode	Authenticated 👻		
-	TFTP Encrypted Co	nfig		
	Phone Security Prof	ile CAPF Information		
	Authentication Mode*	By Existing Certificate (precedence to LSC)		
	Key Size (Bits)*	1024 🗸		
	Note: These fields are	related to the CAPF Information settings on the Phone Configura		

在安全殼層(SSH)作業階段中輸入**utils capf csr count**指令,確認是否已產生CSR。(此螢幕截 圖顯示已為三部電話產生CSR。)



附註:電話的CAPF部分下的證書操作狀態保持為操作掛起。

將產生的CSR從CUCM獲取到FTP(或TFTP)伺服器

1. 通過SSH連線到CUCM伺服器。

2. 執行utils capf csr dump命令。此螢幕抓圖顯示轉儲正在傳輸到FTP。



3. 使用WinRAR開啟轉儲檔案並將CSR提取到本地電腦。



獲取電話證書

1. 將電話的CSR傳送到CA。

2. CA會提供已簽名的憑證。

附註:您可以使用Microsoft Windows 2003 Server作為CA。稍後將說明使用Microsoft Windows 2003 CA簽署CSR的程式。

將.cer轉換為.der格式

如果收到的證書是.cer格式,則將其重新命名為.der。

🔄 SEPD0574CF6BD0F.cer	1/22/2015 3:03 AM	Security Certificate	2 KB
🔄 SEPB83861583BB9.cer	1/22/2015 3:03 AM	Security Certificate	2 KB
SEP1C17D341FD21.cer	1/22/2015 3:00 AM	Security Certificate	2 KB
SEPD0574CF6BD0F.der	1/22/2015 3:03 AM	Security Certificate	2 KB
SEPD0574CF6BD0F.der	1/22/2015 3:03 AM 1/22/2015 3:03 AM	Security Certificate Security Certificate	2 KB 2 KB

將證書(.der)壓縮為.tgz格式

您可以使用CUCM伺服器的根(Linux)來壓縮證書格式。也可以在正常的Linux系統中執行此操作。

1. 使用SFTP伺服器將所有已簽名的證書傳輸到Linux系統。

[root@cm1052_download]#
[root@cm1052 download]# sftp cisco@10.65.43.173
Connecting to 10.65.43.173
cisco@10.65.43.173's password:
Hello, I'm freeFTPd 1.0sftp>
sftp> get *.der
Fetching /SEP1C17D341FD21.der to SEP1C17D341FD21.der
/SEP1C17D341FD21.der 100% 108
Fetching /SEPB83861583BB9.der to SEPB83861583BB9.der
/SEP883861583BB9.der 100% 1098
Fetching /SEPD0574CF6BD0F.der to SEPD0574CF6BD0F.der
/SEPD0574CF6BD0F.der 100% 108*
sftp>
sftp>
sftp> exit
[root@cm1052 download]# 1s
cm-locale-de_DE-10.5.2.1000-1.cop.sgn.md5 copstart.sh SEP1C17D341FD21.der SEPD0574CF6BD0F.der
cm-locale-de_DE-10.5.2.1000-1.tar phonecert SEPB83861583BB9.der
[root@cm1052_download]#

2. 輸入以下命令可將所有.der憑證壓縮到.tgz檔案中。



將.tgz檔案傳輸到SFTP伺服器

完成螢幕抓圖中所示的步驟,以便將.tgz檔案傳輸到SFTP伺服器。



將.tgz檔案匯入CUCM伺服器

- 1. 通過SSH連線到CUCM伺服器。
- 2. 執行utils capf cert import命令。



成功匯入證書後,您可以看到CSR計數變為零。



使用Microsoft Windows 2003證書頒發機構簽署CSR

這是Microsoft Windows 2003 - CA的可選資訊。

1. 開啟證書頒發機構。



2. 按一下右鍵CA並導航到**所有任務>提交新請求……**

📴 Certification Authority	
<u>File Action View H</u> elp	
	⅔ 💵 ▶ 🔳
Entification Authority (Local)	Name
AMEER-CA_	Revoked Certificates
	Start Service
Issued	Stop Service
Pendin View	
Failed Refresh	Submit <u>n</u> ew request
Export List	Back up CA
	Restore CA
P <u>r</u> operties	
	Rene <u>w</u> CA Certificate

3. 選擇CSR,然後按一下**Open**。對所有CSR執行此操作。



所有開啟的CSR都會顯示在「暫掛請求」資料夾中。

4. 按一下右鍵每個任務並導航到**所有任務>發出**以發出證書。對所有掛起請求執行此操作。



- 5. 若要下載憑證,請選擇Issued Certificate。
- 6. 按一下右鍵證書,然後按一下Open。

📴 Certification Authority				_ 🗆 🗵
<u>File Action View H</u> elp				
E Certification Authority (Local)	Request ID	Requester Name	Binary Certificate	Serial Numl 🔺
🖻 👩 AMEER-CA	30	DATA-SRV225\A	BEGIN CERTI	11cd7e360
Revoked Certificates	31	DATA-SRV225\A	BEGIN CERTI	11cf86c70
Issued Certificates	32	DATA-SRV225\A	BEGIN CERTI	11d088d60
Pending Requests	33	DATA-SRV225\A	BEGIN CERTI	11af75cb0
Failed Requests	34	DATA-SRV225\A	BEGIN CERTI	11af83490
	🚟 35	DATA-SRV225\A	BEGIN CERTI	11af8e450
	36	Open	BEGIN CERTI	122267260
	37	A	BEGIN CERTI	122272900
	38	All Tasks 🕨 A	BEGIN CERTI	12227c920
	•	Refresh		•
Open this item		Help		

7. 您可以檢視證書詳細資訊。若要下載憑證,請選擇「詳細資訊」索引標籤,然後選擇**「複製到** 檔案……」

Certi	icate ?	×
Gei	eral Details Certification Path	1
	Certificate Information	
	This certificate is intended for the following purpose(s): •All application policies	
	Issued to: SEP1C17D341FD21	
	Issued by: AMEER-CA	
	Valid from 1/22/2015 to 1/22/2016	
	Issuer Statement	
	OK	

8. 在「Certificate Export Wizard(證書匯出嚮導)」中,選擇**DER encoded binary** X.509(.CER)。

show: <all></all>	<u> </u>	Certificates can be exported in a variety of file formats.
Pield Version Serial number Signature algorithm Issuer Valid from Valid from Valid to Subject Public key	Value * V3 12 22 67 26 00 00 00 00 00 24 sha1RSA AMEER-CA Thursday, January 22, 2015 2 Friday, January 22, 2016 2:51 SEP1C17D341FD21, ourm, cis RSA (2048 BRs)	Select the format you want to use: DER encoded binary X.509 (.CER): Bage-64 encoded X.509 (.CER): Dyptographic Message Syntax Standard - PKCS #7 Certificates (.P78) Include all certificates in the certification path if possible Dersonal Information Exchange - PKCS #12 (.PFX) Include all certificates in the certification path if possible Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above) Delste the private lay if the export is successful
	Edit Properties	ECGIN CERTI 122272901 EEGIN CERTI 122272901

9. 為檔案命名適當的名稱。此示例使用<MAC>.cer格式。

e to Evnort	
Specify the name of the file you want t	o export
<u>F</u> ile name:	

10. 通過此過程,在「已頒發的證書」部分下獲取其他電話的證書。

從CA取得根憑證

1. 開啟證書頒發機構。

2. 完成此熒幕截圖所示的步驟即可下載根CA。

Test. pcop Ele Action Authority Ele Action Yew AMEER-CA Properties Certificate Managers Restrictions General Policy Module Evit Mo Certificate	Auditing Security adule Extensions Storage	Certificate General Détais Certification Show: <al></al>	Path	? ×
and click on properties Certificate Information This certificate is intended for the following purpose(s): •Al issuance policies •Al application policies	3 View Certificate	Field Version Serial number Signature algorithm Lissuer Valid from Valid to Subject Public key	Value V3 12 96 ad 39 4c 29 97 a0 45 c5. shaIRSA AMEER-CA Tuesday, May 07, 2013 8:55: Monday, May 07, 2018 9:02:4. AMEER-CA RSA (2048 Bbs)	
Issued to: AMER-CA Issued by: AMER-CA Valid from 5/7/2013 to 5/7/2018	Uptographic Provider		5 Edit Properties Copy to Fi	e
Issuer Batement				ок

驗證

使用本節內容,確認您的組態是否正常運作。

- 1. 轉到電話配置頁面。
- 2. 在CAPF部分下,證書操作狀態應顯示為**升級成功**。

certificate operation	No Pending Operation	•
Authentication Mode*	By Existing Certificate (precedence to LSC)	
uthentication String		
Generate String		
(ey Size (Bits)*	1024	
Operation Completes By	2015 1 24 12 (YYYY:MM:DD:HH)	
Certificate Operation Status	s: Upgrade Success	

附註:如需詳細資訊,請參閱產生和匯入第三方CA簽署的LSC。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。