在UCSM上建立和使用第三方證書

目錄		
<u>簡介</u>		
<u>必要條件</u>		
<u>需求</u>		
<u>採用元件</u>		
<u>設定步驟</u>		
配置信任點		
<u>步驟 1</u>		
<u>步驟 2</u>		
<u>步驟 3</u>		
<u>建立金鑰環和CSR</u>		
<u>步驟 1</u>		
<u>步驟 2</u>		
<u>步驟 3</u>		
<u>步驟 4</u>		
應用金鑰環		
<u>步驟 1</u>		
相關資訊		

簡介

本文描述在統一計算系統(UCS)上建立和使用第三方證書以進行安全通訊的過程。

必要條件

需求

思科建議您瞭解以下主題:

- 訪問CA授權
- UCSM 3.1

採用元件

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。

設定步驟

配置信任點

步驟 1

- 從CA授權機構下載證書鏈以建立信任點。請參閱證書伺服器中的 <u>http://localhost/certsrv/Default.asp</u>。
- 確保編碼設定為Base 64。

Microsoft Active Directory Certificate Services - Enterprise CA-1	• Recording	00:06:21	П	
Download a CA Certificate, Certificate Chain, or CRL				
To trust certificates issued from this certification authority, install this CA certificate.				
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.				
CA certificate: Current [Enterprise CA-1(1)]				
Encoding method: O DER @ Base 64) () ÷
Install CA certificate Download CA certificate Download latest base RL Download latest delta CRL				2°.

從CA授權機構下載憑證鏈結

步驟 2

• 下載的憑證鏈結為PB7格式。



- 使用OpenSSL工具將.pb7檔案轉換為PEM格式。
- 例如,在Linux中,您可以在終端機中執行此指令,以執行轉換- openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem。

步驟 3

- 在UCSM上建立信任點。
- 導航到Admin > Key Management > Trustpoint。
- 建立信任點時,在證書詳細資訊空間中貼上本部分步驟2中建立的.PEM檔案的完整內容。



建立金鑰環和CSR

步驟 1

- 導航到UCSM > Admin > Key Management > Keyring。
- 選擇第三方證書所需的模數。

Key Ring

Name :	3rd-party	
Modulus :	○ Mod2048 ○ Mod2560 ○ Mod3072 ○ Mod3584	Mod4096

步驟 2

- 按一下create certificate request, 並填寫請求的詳細資訊。
- 複製請求欄位的內容。



步驟 3

若要產生憑證,請將步驟2中複製的要求貼到下方空白處:

Microsoft Active Directory Certificate Services - Enterprise CA-1

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 the Saved Request box.

Saved Request:				
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	<		~	
Certificate Templ	ate: User - ING		_	
Additional Attribu	ites:			
Attributes:		~		
		Submit	:>	

步驟 4

 • 提交後,將生成新證書。打開檔案並複製本部分步驟1中建立的金鑰環上的證書欄位中新生成 的證書的所有內容。

rusted Point :	Trust-test	T
Certificate :	BEGIN CERTIFICA MIIGLJCCBRagAwIBAgI 9w0BAQsFADBIMRgwF CZImiZPyLGQBGRYIaW ZAEZFgJJTjEYMBYGA1 AxMPRW50ZXJwcmIzZ	TE KS4anFAABAAa9jDANBgkqhkiG gYK 50cmFuZXQxEjAQBgoJkiaJk/Is UE SBDQS0xMB4XDTE4MDUwOD

• 從建立金鑰環和CSR的步驟3中建立的下拉選單中選擇信任點。

應用金鑰環

步驟 1

選擇通訊服務中建立的金鑰環,如下所示:

cisco	UCS Manager	
ж	All	All / Communication Management / Communication Services
-	 Locally Authenticated Users Remotely Authenticated Users Roles 	Communication Services Events FSM Redirect HTTP to HTTPS :
≢	 Key Management KeyRing default KeyRing Test Keyring 	Admin State : Enabled Disabled
	KeyRing ucsm_5108	Admin State : Enabled Disabled
	TP root TP Trust-test	Port : 443 Operational Port : 443
20	 Communication Management Call Home 	Cipher Suite Mode : High Strength Medium Strength Low Strength Custom
	Communication Services DNS Management Management Interfaces	Allowed SSL Protocols : Allow all except SSLv2 and SSLv3) Only TLSv1.2 CIM XML

更改金鑰環後,與UCSM的HTTPS連線在Web瀏覽器中顯示為安全。



注意:這需要本地案頭也使用與UCSM來自同一CA機構的證書。



相關資訊

• <u>技術支援與文件 - Cisco Systems</u>

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)。