在UCSM上创建和使用第三方证书

目录		
<u>先决条件</u>		
<u>要求</u>		
<u>使用的组件</u>		
<u>配置步骤</u>		
配置信任点		
<u>第1步</u>		
<u>步骤 2</u>		
<u>步骤 3</u>		
<u>创建密钥环和CSR</u>		
<u>第1步</u>		
<u>步骤 2</u>		
<u>步骤 3</u>		
<u> </u>		
<u>应用密钥环</u>		
<u> </u>		
<u>相天信息</u>		

简介

本文档介绍在Unified Computing System (UCS)上创建和使用第三方证书以进行安全通信的步骤。

先决条件

要求

Cisco 建议您了解以下主题:

- 访问CA颁发机构
- UCSM 3.1

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

配置步骤

配置信任点

第1步

- 从CA机构下载证书链以创建Trust-Point。请参阅证书服务器中的 <u>http://localhost/certsrv/Default.asp</u>。
- 确保编码设置为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: ODER @Base 64				0
Install CA certificate Download CA certificate Download latest base CRL Download latest delta CRL				***

从CA颁发机构下载证书链

步骤 2

• 下载的证书链为PB7格式。



- 使用OpenSSL工具将.pb7文件转换为PEM格式。
- 例如,在Linux中,您可以在终端中运行此命令以执行转换- openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem。

步骤 3

- 在UCSM上创建信任点。
- 导航到Admin > Key Management > Trustpoint。
- 创建信任点时,将本部分步骤2中创建的.PEM文件的完整内容粘贴到证书详细信息空间中。



创建密钥环和CSR

第1步

- 导航到UCSM > Admin > Key Management > Keyring。
- 选择第三方证书所需的模数。

Key Ring

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

步骤 2

- 单击create certificate request,并填写请求的详细信息。
- 复制请求字段的内容。



步骤 3

要生成证书,请将步骤2中复制的请求粘贴到下面显示的空白处:

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:				
Additional Attribu	ites:				
Attributes:	<	>			
		Subr	nit >		

步骤 4

 • 提交后,将生成新证书。打开文件并复制本部分步骤1中创建的密钥环上证书字段中新生成的 证书的所有内容。

Trusted Point :	Trust-test	Ψ.	
Certificate :	BEGIN CERT MIIGLJCCBRagAw 9w0BAQsFADBIM CZImiZPyLGQBGI ZAEZFgJJTJEYMB AxMPRW50ZXJw	TIFICATE IBAgIKS4anFAABA/ IRgwFgYK RYIaW50cmFuZXQx IYGA1UE cmIzZSBDQS0xMB4	jDANBgkqhkiG QBgoJkiaJk/Is)TE4MDUwOD

• 从创建密钥环和CSR的步骤3中创建的下拉列表中选择信任点。

应用密钥环

第1步

选择通信服务中创建的密钥环,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 : Enabled Disabled
≣	✓ Key Management KeyRing default	Admin State : Enabled Disabled
Q	KeyRing Test_Keyring KeyRing ucsm_5108	Admin State : Enabled Disabled
	TP root TP Trust-test	Port : 443 Operational Port : 443 Key Ring : KeyRing Test Keyring T
1 ₀	 Communication Management Call Home 	Cipher Suite Mode : High Strength Medium Strength Low Strength Custom
	Communication Services DNS Management Management Interfaces	Allowed SSL Protocols : Odefault (Allow all except SSLv2 and SSLv3) Only TLSv1.2

更改密钥环后,到UCSM的HTTPS连接在Web浏览器中显示为安全。



注意:这要求本地桌面也使用与UCSM相同的CA机构颁发的证书。



相关信息

• <u>技术支持和文档 - Cisco Systems</u>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。