CUCM第三方CA签名LSC生成和导入配置示例

目录

简介 先决条件 要求 使用的组件 配置 上传CA根证书 为终端证书颁发设置脱机CA 为电话生成证书签名请求(CSR) 获取从CUCM到FTP(或TFTP)服务器的生成的CSR 获取电话证书 将.cer转换为.der格式 将证书(.der)压缩为.tgz格式 将.tgz文件传输到SFTP服务器 将.tgz文件导入CUCM服务器 使用Microsoft Windows 2003证书颁发机构签署CSR 从CA获取根证书 验证 故障排除

简介

证书授权代理功能(CAPF)本地重要证书(LSC)是本地签名的。但是,您可能需要电话使用第三方证 书颁发机构(CA)签名的LSC。本文档介绍可帮助您实现这一点的过程。

先决条件

要求

思科建议您了解思科统一通信管理器(CUCM)。

使用的组件

本文档中的信息基于CUCM 10.5(2)版;但是,此功能在10.0版及更高版本中有效。

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。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

配置

下面是此过程所涉及的步骤,每个步骤都在其自己的部分中进行了详细说明:

- 1. 上传CA根证书
- 2. <u>为终端证书颁发设置脱机CA</u>
- 3. <u>为电话生成证书签名请求(CSR)</u>
- 4. <u>从Cisco Unified Communications Manager(CUCM)获取生成的CSR到FTP服务器</u>
- 5. <u>从CA获取电话证书</u>
- 6. <u>将.cer转换为.der格式</u>
- 7. <u>将证书(.der)压缩为.tgz格式</u>
- 8. <u>将.tgz文件传输到Secure Shell FTP(SFTP)服务器</u>
- 9. <u>将.tgz文件导入CUCM服务器</u>
- 10. 使用Microsoft Windows 2003证书颁发机构签署CSR
- 11. <u>从CA获取根证书</u>

上传CA根证书

- 1. 登录思科统一操作系统(OS)管理Web GUI。
- 2. 导航到安全证书管理。
- 3. 单击Upload Certificate/Certificate chain。
- 4. 在Certificate Purpose下选择CallManager-trust。
- 5. 浏览到CA的根证书,然后单击Upload。

cisco U For Cisco U	nified Operating System Administration
Show - Settings - Sec	urity 🔻 Software Upgrades 👻 Services 👻 Help 👻
🕹 Upload Certificate/Certi	icate chain - Mozilla Firefox
https://10.106.122.173/	cmplatform/certificateUpload.do
Upload Certificate/Ce	rtificate chain
Upload Lose	
Status Warning: Uploadir	g a cluster-wide certificate will distribute it to all servers in this cluster
Upload Certificate/C	ertificate chain
Certificate Purpose*	CallManager-trust
Description(friendly na	me)
Upload File	Browse AMEER-CA.cer
Upload Close	

为终端证书颁发设置脱机CA

- 1. 登录到CUCM管理Web GUI。
- 2. 导航到System > Service Parameter。
- 3. 选择CUCM Server并为服务选择Cisco Certificate Authority Proxy Function。
- 4. 选择Offline CA以向终端颁发证书。

diala	Cisco Unified CM Administration	
	For Cisco Unified Communications Solutions	
System 🖣	Call Routing 👻 Media Resources 👻 Advanced Features 👻 Dev	rice 👻 Application 👻 User Mana <u>c</u>
Service Pa	rameter Configuration	
Save	Set to Default	
Status		
Status		
(i) Status	: Ready	
Select Se	rver and Service	
Server*	10 106 122 173CUCM Voice/Video (Active)	
Service*		
Service	Cisco Certificate Authority Proxy Function (Active)	
All parame	ters apply only to the current server except parameters tha	t are in the cluster-wide group(s
Cisco Cer	ificate Authority Proxy Function (Active) Parameters	s on server 10.106.122.173
Parameter	Name	Parameter Value
Certificate	Issuer to Endpoint *	Offline CA
Duration O	f Certificate Validity	5
Key Size *		1024
Maximum /	Allowable Time For Key Generation *	30
Maximum A	Allowable Attempts for Key Generation *	3

为电话生成证书签名请求(CSR)

- 1. 登录到CUCM管理Web GUI。
- 2. 导航到**设备电话**。
- 3. 选择其LSC必须由外部CA签名的电话。
- 4. 将设备安全配置文件更改为安全配置文件(如果不存在,请在安全电话安全配置文件上添加一 个系统)。
- 5. 在电话配置页面的CAPF部分下,选择**Install/Upgrade**进行认证操作。对于其LSC必须由外部 CA签名的所有电话,请完成此步骤。对于证书操作状态,您应该看到**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		

Certificate Operation*	Install/Upgrade	•
Authentication Mode*	By Null String	•
Authentication String		
Generate String		
Key Size (Bits)*	2048	•
Operation Completes By	2015 1 24 12 (YYYY:MM:DD:HH)	
Certificate Operation Statu	s: Operation Pending	
Note: Security Profile Conta	ains Addition CAPF Settings.	

电话安全配置文件(7962型号)。

Phone Security Prof	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

在安全外壳(SSH)会话中输入**utils capf csr count**命令以确认是否生成CSR。(此屏幕截图显示 已为三部电话生成CSR。)



注意:电话的CAPF部分下的证书操作状态仍处于操作挂起状态。

获取从CUCM到FTP(或TFTP)服务器的生成的CSR

1. 通过SSH连接到CUCM服务器。

2. 执行utils capf csr dump命令。此屏幕截图显示正在传输到FTP的转储。



3. 使用WinRAR打开转储文件并将CSR提取到本地计算机。



获取电话证书

1. 将电话的CSR发送到CA。

2. CA为您提供签名证书。

注意:您可以使用Microsoft Windows 2003服务器作为CA。使用Microsoft Windows 2003 CA签署CSR的过程将在本文档后面部分说明。

将.cer转换为.der格式

如果收到的证书是.cer格式,则将其重命名为.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

将证书(.der)压缩为.tgz格式

可以使用CUCM服务器的根(Linux)压缩证书格式。也可以在正常的Linux系统中执行此操作。

1. 将所有签名证书通过SFTP服务器传输到Linux系统。

[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% 1087
Fetching /SEPB83861583BB9.der to SEPB83861583BB9.der
/SEPB83861583BB9.der 100% 1095
Fetching /SEPD0574CF6BD0F.der to SEPD0574CF6BD0F.der
/SEPD0574CF6BD0F.der 100% 1087
sftp>
sftp>
sftp> exit
[root@cm1052 download]# 18
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. 输入此命令以将所有.der证书压缩为.tgz文件。

tar -zcvf



将.tgz文件传输到SFTP服务器

完成屏幕截图中所示的步骤,将.tgz文件传输到SFTP服务器。

[root@cm1052 download]#	sftp cisco@10.65.43.173					
Connecting to 10.65.43.1	Connecting to 10.65.43.173					
cisco@10.65.43.173's password:						
Hello, I'm freeFTPd 1.0s	ftp>					
sftp>						
sftp> put phoneDER.tgz						
Uploading phoneDER.tgz t	o /phoneDER.tgz					
phoneDER.tgz						
sftp>						

将.tgz文件导入CUCM服务器

- 1. 通过SSH连接到CUCM服务器。
- 2. 执行utils capf cert import命令。



成功导入证书后,您可以看到CSR计数变为零。



使用Microsoft Windows 2003证书颁发机构签署CSR

这是Microsoft Windows 2003 - CA的可选信息。

1. 打开证书颁发机构。



2. 右键单击CA并导航到**所有任务>提交新请求……**

📴 Certification Au	Ithority		
Eile <u>A</u> ction <u>V</u> iew	w <u>H</u> elp		
⇔ ⇒ 🗈 💽	e 0 6	ß	? ⊡ ▶ ■
Certification Aut	hority (Local)		Name
🖻 🕝 AMEER-CA			Revoked Certificates
Revok	All Tas <u>k</u> s	•	Start Service
- 📄 Issued			Stop Service
- Pendin	View	1	
Failed	Refresh		Submit <u>n</u> ew request
	Export List		Back up CA
			Bestore C0
	Properties		Restore CA
		_	Renew CA Certificate
	Help	-	

3. 选择CSR并单击Open。对所有CSR执行此操作。



所有打开的CSR都会显示在"待处理请求"文件夹中。

4. 右键单击每个任务并导航到**所有任务>发出**以颁发证书。对所有挂起请求执行此操作。



- 5. 要下载证书,请选择Issued Certificate。
- 6. 右键单击证书,然后单击打开。

📴 Certification Authority				_ 🗆 🗵
Eile <u>A</u> ction <u>V</u> iew <u>H</u> elp				
E Certification Authority (Local)	Request ID	Requester Name	Binary Certificate	Serial Numl 🔺
E MEER-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
	28 36	Onen A	BEGIN CERTI	122267260
	37	A	BEGIN CERTI	122272900
	38	All Tas <u>k</u> s ► A	BEGIN CERTI	12227c920
	•	Re <u>f</u> resh		•
Open this item		Help		

7. 您可以查看证书详细信息。要下载证书,请选择Details选项卡,然后选择Copy to File...

Certi	ficate	? ×
Ger	neral 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	
L	Issuer Stateme	nt
	0	<

8. 在Certificate Export Wizard中,选择DER encoded binary X.509(.CER)。

how: <al></al>	×	
Field Version Serial number Signature algorithm Issuer Valid from Valid from Subject Public key	Value V3 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 SEP1C17D341F021, outm, ds RSA (2048 Bts) ¥	Select the format you want to use:
	Edit Properties	<back mext=""> Cancel -BEGIN CERTI 122272900 -BEGIN CERTI 122276920 •</back>

9. 为文件命名适当的名称。本示例使用<MAC>.cer格式。

icate export wizaru	
le to Export	
Specify the name of the file you want to export	
Eile name:	
TA\CA\RameshCUCM\LABPhoneCSR\CER\SEP1C17D341FD21.cer	Browse

10. 通过此过程在Issued Certificate部分下获取其他电话的证书。

从CA获取根证书

- 1. 打开**证书颁发机构**。
- 2. 完成此屏幕截图中所示的步骤,以下载根CA。

Test, pcap Efe Action Authority Efe Action View AMEER-CA Properties Certificate Managers Restrictions Certificate Managers Restrictions Efficient Policy Module Exit Mo Certificate CA Certificate View Certificate View	Auditing Security dule Extensions Storage	Certificate General Details Certification	X
General [Details] Certification 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 Issuer Veld from Veld to Subject Public key	Value V3 12 96 ad 39 4c 29 97 a0 45 c5 shaIRSA AMEER-CA Tuesday, May 07, 2018 9:02:4 AMEER-CA RSA (2048 Bits)
Issued to: AMEER-CA Issued by: AMEER-CA Valid from 5/7/2013 to 5/7/2018	leptographic Provider		5
Issuer 2 atoment			Edit Properties Copy to Fie

验证

使用本部分可确认配置能否正常运行。

- 1. 转到电话配置页面。
- 2. 在CAPF部分下,证书操作状态应显示为**升级成功**。

By Existing Certificate (precedence to LSC)	
24	
15 1 24 12 (YYYY:MM:DD:HH)	
rade Success	

注意:有关详细信息,请参阅<u>生成和导入第三方CA签名的LSC</u>。

故障排除

目前没有针对此配置的故障排除信息。