配置Finesse和CTI服务器之间的安全通信

目录

简介 先决条件 要求 使用的组件 背景信息 配置 CCE CTI服务器安全 Finesse安全配置 生成代理PG证书(CTI服务器) 获取CA签名的CSR证书 导入CCE PG CA签名的证书 生成Finesse证书 通过CA签署Finesse证书 导入Finesse应用和根签名证书 验证 故障排除

简介

本文档介绍如何在Cisco Contact Center Enterprise(CCE)解决方案中在Cisco Finesse和计算机电话 集成(CTI)服务器之间实施证书颁发机构(CA)签名证书。

先决条件

要求

Cisco 建议您了解以下主题:

- CCE版本12.0(1)
- Finesse版本12.0(1)
- CTI服务器

使用的组件

本文档中的信息基于以下软件版本:

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

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。

背景信息

在CCE 11.5版中,思科开始支持传输层安全(TLS)版本1.2,这允许会话初始协议(SIP)和实时传输协 议(RTP)消息通过TLS 1.2安全地传输。从CCE 12.0并作为保护数据的一部分在移动中,思科开始在 大多数联系中心呼叫流上支持TLS 1.2:入站和出站语音、多通道和外部数据库下滑。本文档重点介 绍入站语音,尤其是Finesse和CTI服务器之间的通信。

CTI服务器支持以下连接模式:

- **仅安全连接**:允许在CTI服务器和CTI客户端(Finesse、拨号器、CTIOS和ctitest)之间进行安全 连接。
- **安全和非安全连接(混合模式):**允许CTI服务器和CTI客户端之间的安全连接以及非安全连接 。这是默认连接模式。当您将以前版本升级到CCE 12.0(1)时,将配置此模式。

注意: 不支持非安全仅模式。

配置

CCE CTI服务器安全

步骤1.在PCCE管理工作站(AW)上,打开Unified CCE Tools文**件夹,**然后双击Peripheral Gateway Setup**(外围设备网关设置)**。



步骤2.选择CG3A并单击"编辑"。

Cisco Unified ICM/Contact Ce	enter Enterprise Components Setup
ICM Instances Add Edit Delete To set up Administration Data Server (D Interface Controller (NIC), WebView of Web Setup tool. To set up Administration Client (Client A and Setup tool. The Instance cc cannot be deleted be Web Setup tool.	Instance Components Add PG1A PG1A PG2A PG3A PG3A RoutesA Delete Delete Delete Delete Notwork Gateway components, use the W), use the Administration Client Installer cause it has components set up by the up tool. You must use the applicable tool steing the instance in Peripheral Gateway
	Help Exit Setup

步骤3.在CTI服务器属性上,单击Next。有关设置停止CG3A服务的问题,请选择是。

步骤4.在CTI Server Components Properties(CTI服务器组件属性)中,选择Enable Secured-only mode(启用仅安全模式)。</mark>请注意安**全连接端口(46030)**,因为在下一练习中,您必须在Finesse中 配置同一端口。单击 Next。

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

注意:默认安全通信是42030,但本文档使用的实验是40630。端口号是包含ICM系统ID的公式的一部分。当系统ID为1(CG1a)时,默认端口号通常为42030。由于实验中的系统ID为3(CG3a),因此默认端口号为46030。

步骤5.在"CTI网络**接口属性"上,**单击"下**一步"**。选中"Setup **Information(设置信**息)" ,然**后单击 "Next**(下一步)"。

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:\jicm	=
Configuration: PG node is pocealin1p CTI Gateway is simplexed DMP address is 3	-
<	>
InstaliShield	
< Back Next >	Cancel

步骤6.单击"完**成"**,如图所示。

Unified 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/ICC Node Manager Click Finish to Complete Setup.		
< Back Finish Cancel			

步骤7.单击"退**出设置**",然后等待安装窗口关闭,如图所示。

ICM Instances	Instance Comp	onents
ce	AW	644
	LoggerA	MOG
	Edit PG1A	Edit
	PG3A	
	Delete Route:A	Delete
To set up Administration D Interface Controller (NIC).	Data Server (Distributor AW), Rout WebView or Network Gateway c	er, Logger, Network proponents, use the
To set up Administration D Interface Controller (NIC), Web Setup tool. To set up Administration D and Setup tool.	Data Server (Distributor AW), Rout WebView or Network Gateway of Dient (Client AW), use the Adminis	er, Logger, Network omponents, use the sation Client Installer
To set up Administration D Interface Controller (NIC), Web Setup tool. To set up Administration O and Setup tool. The Instance cc cannot I Web Setup or Administrat to remove those compone Setup.	Data Server (Distributor AW), Rout WebView or Network Gateway of Client (Client AW), use the Adminis be deleted because it has compor tion Client Setup tool. You must us ents before deleting the instance in	er, Logger, Network omponents, use the sation Client Installer ents set up by the e the applicable tool h Peripheral Gateway

步骤8.在PCCEAllin1桌面上,双击Unified CCE**服务控制**。

步骤9.选择Cisco ICM cc CG3A并单击"开始"。

Finesse安全配置

步骤1.打开Web浏览器并导航至Finesse Administration。

步骤2.向下滚动到Contact Center Enterprise CTI Server Settings(联系中**心企业CTI服务器设置)部** 分,如图所示。

Contact Center Ent	erprise CTI Server S	Settings	
Note: Any changes made to Contact Center Enterpris	the settings on this gadget se 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*	42027	B Side Port	
Peripheral ID*	5000		
Enable SSL encryption Save Reve	rt -		

步骤3.在上一练习中,更改CG3A上配置的安全通信端口的A侧端口:**46030。选**中"启**用SSL加密"**并 单击"**保存"**。

Contact Center Ent	erprise CTI Server Se	attings	
Note: Any changes made to Contact Center Enterpris	the settings on this gadget in se CTI Server Settings	equire a restart of Cisco Finesse Torncat to	take effect.
A Side Host/IP Address*	10.10.10.10	8 Side Host/IP Address	
A Side Port*	46030	B Side Port	
Peripheral ID*	5000	1	
Enable SSL encryption	rt		

注意: 要测试连接,您需要先重新启动Finesse Tomcat服务或重新启动Finesse服务器。

步骤4.从Finesse Administration页面注销。

步骤5.打开与Finesse的SSH会话。

步骤6.在FINESSEA SSH会话上,执行命令:

utils system restart

当系统询问您是否要重新启动系统时,输入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证书(CTI服务器)

CiscoCertUtils是CCE版本12上发布的新工具。您使用此工具管理入站语音的所有CCE证书。在本 文档中,您使用这些CiscoCertUtils来生成外围网关(PG)证书签名请求(CSR)。 步骤1.执行此命令以生成CSR证书: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\keys\host.key. It will be used to generate the CSR. SYSTEM command is C:\icm\ssl\keys\host.cfg SYSTEM command is C:\icm\ssl\keys\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.

提供所请求的信息,例如:

国家/地区名称:美国

省/自治区名称:MA

位置名称:BXB

单位名称: 思科

组织单位:CX

公用名: PCCEAllin1.cc.lab

邮件:jdoe@cc.lab

质询密码:火车!

可选公司名称: 思科

主机证书和密钥存储在C:\icm\ssl\certs和C:\icm\ssl\keys。

步骤2.导航至C:\icm\ssl\certs文件夹,并确保已生成该文件host.csr。

获取CSR证书 由CA签名

生成CSR证书后,需要由第三方CA签名。在本练习中,域控制器中安装的Microsoft CA用作第三方CA。

确保CA使用的证书模板包括客户端和服务器身份验证,如使用Microsoft CA时的映像所示。

Properties of New Template	pns	
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 Edk. Extensions included in this template:	tificate Templates More Actions b Server More Actions	(DC.cc.lab)
Application Policies	An application policy defi	Add Application Policy
Certificate Template Information	Application policies:	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.
Edt Description of Application Policies:		Any Purpose Attestation Identity Key Certificate Certificate Request Agent Element Authentication
Server Authentication	Add	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
OK Cancel Apply Help		OK Cancel

步骤1.打开Web浏览器并导航至CA。

步骤2.在Microsoft Active Directory证**书服务上,选**择请**求证书**。

_ O X
🗲 💿 🧭 https://dc.cc.lab/certini/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

步骤3.选择高级证**书请求**选项。

Micr	osoft Activ	e Directory Ce	ertifica × +				
\leftrightarrow	C' ŵ		🛈 🔒 https://dc.	c.lab/certsrv/en	-us/certr	qus.asp	
🗎 СИСМ	🛅 CUIC	🛅 Finesse	🛅 Remote Expert Mobile	🛅 MediaSense	CVP	CCE	8
Request	a Certif	icate	cate Genices - CC-OC-C	~^			
	a and the	ata tuma:					

步骤4.在高级证书请求上,复制并粘贴PG代理CSR证书的内容到"已保存的请求"框。

步骤5.选择带客户端**和服务器**身份验证的Web服务器模板。在实验中,CC Web Server模板是使用 客户端和服务器身份验证创建的。

Microsoft Active	Directory Certificate Services – cc-DC-CA
Submit a Cert	ificate Request or Renewal Request
To submit a sar Saved Reques	t box. Copy and paste the contents of the expected CSR file
Saved Request:	
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	3LhnlD3GsLbIYivb7lbshWfqH1509jMcZ3uZrciC ^ gNL/H3DR1nRpJtLKfnLGgX5kUAZqin/56HjuGb4h + +L3E0yNQ+W9/SJojYzBGnHk38yo1P/I7UsueE30R J75nKDoyAh7C+F0u9tmg26DZa0Z3k9Wo5QzUTPmd rArT900dxJem - END CERTIFICATE REQUESTsna >
Certificate Temp	late:
	CC Web Server
Additional Attrib	utes:
Attributes:	je.
	Submit >

步骤6.单击"提**交"**。

步骤7.选择Base 64编码,然后单击Download Certificate,如图所示。

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

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

-	-			
17	2	2	5	¢.
	9	2	7	9
12	2	2	2	2

Download certificate Download certificate chain

步骤8.保存文件并单击"确定"。文件保存在"下载"文件夹中。

步骤9.将文件重命名**为host.cer**(可选)。

步骤10.您还需要生成根证书。返回CA证书页面,然后选择**Download a CA certificate, certificate chain, or CRL**。您只需执行此步骤一次,因为根证书对所有服务器(PG代理和Finesse)都是相 同的。

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

Welcome

Use this Web site to request a certificate for your Web browser, ϵ people you communicate with over the Web, sign and encrypt m-security tasks.

You can also use this Web site to download a certificate authority status of a pending request.

For more information about Active Directory Certificate Services,

Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>

步骤11.单击Base 64并选择"下载CA证书"。

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

步骤12.单击Save File(保存文件)并选择OK(确定)。文件将保存在默认位置"Downloads"中。

导入CCE PG CA签名的证书

步骤1.在PG代理上导航至C:\icm\ssl\certs,并将根文件和PG代理签名文件粘贴到此处。

步骤2.将c:\icm\ssl\certs 上的host.pem证书重命名为selfhost.pem。

步骤3.将host.cer重命名为c:\icm\ssl\certs 文件夹上的host.pem。

步骤4.安装根证书。在命令提示符下,发出以下命令:CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer



第五步: 安装运行相同命令的应用程序签名证书: CiscoCertUtil /install C:\icm\ssl\certs\host.pem



步骤6.循环PG。打开Unified CCE Service Control,并循环Cisco ICM Agent PG。

生成Finesse证书

步骤1.打开Web浏览器并导航至Finesse OS Admin。

步骤2.使用OS Admin凭据登录,然后导航到Security > Certificate Management,如图所示。



步骤3.单击"生**成CSR"**,如图所示。



步骤4.在生成证**书签名请**求中,使用默认值,然后单击**生成。**

Generate Certificate Si	gning Request
🔒 Generate 🛛 🖳 Close	
61.1.	
Status	
Warning: Generatin	g a new CSR for a specific certificate type will overwrite the existing CSR for that type
Generate Certificate S	Signing Request
Certificate Purpose**	tomcat v
Distribution*	FINESSEA.cc.lab v
Common Name*	FINESSEA.cc.lab
Subject Alternate Nar	mes (SANs)
Parent Domain	cc.lab
Key Type**	RSA
Key Length*	2048 v
Hash Algorithm	SH4256 V
Generate Close	ed item. icate Purpose ending with "-ECDSA" is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it

步骤5.关闭"生成证书签名请求"窗口并选择"下载CSR"。



步骤6.在Certificate Purse(证书用途)中,选择**tomcat并**单击Download CSR**(下载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
(i) *- indicates required item.
< >

步骤7.选择"**保存文**件"并单击"确定",如图所示。

Opening tomcat.csr	×
You have chosen to open:	
tomcat.csr	
which is: csr File	
from: https://finessea.cc.lab:8443	
What should Firefox do with this file?	
O Open with Browse	
Save File	
Do this automatically for files like this from now on	
_ bo ons gutomatically for files like ons from now on.	
OK Cancel	

步骤8.关闭"下载证书签名请求"窗口。证书保存在默认位置(此PC >下载)。

步骤9.打开Windows资源管理器并导航至该文件夹。右键单击此证书并将其重命名 :finsetomcat.csr

通过CA签署Finesse证书

在本节中,上一步中使用的相同Microsoft CA用作第三方CA。

注意: 确保CA使用的证书模板包括客户端和服务器身份验证。

步骤1.打开Web浏览器并导航至CA。

步骤2.在Microsoft Active Directory证**书服务上,选**择请**求证书**。

_ 0 X
🗲 💿 🖉 https://dc.cc.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

步骤3.选择高级证书请求选项,如图所示。

Micr	osoft Activ	e Directory Ce	ertifical × +				
\leftrightarrow	C' û		🛈 🐔 https://dc.c	c.lab/certsrv/en	-us/certr	qus.asp	
CUCM	🛅 CUIC	🛅 Finesse	🛅 Remote Expert Mobile	🛅 MediaSense	CVP	CCE	8
Microsoft Request	Active Dire	ectory Certifi icate	cate Services cc-DC-C	CA			
Select the	e certific	ate type: e					_
Or, subm	it an <u>adv</u>	anced cer	rtificate request.				

步骤4.在高级证书请求上,将Finesse CSR证书的内容复制并粘贴到"已保存的请求"框。

步骤5.选择具有客户端和服务器身份验证的Web服务器模板。在本实验中,CC Web服务器模板是 使用客户端和服务器身份验证创建的。

Microsoft Active	Directory Certificate Services -	cc-DC-CA	
Submit a Certi	ificate Request or Renew	val Request	
To submit a say Saved Request	ved request to the CA, part box.	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+F0u9tmg260 rArT90OdxJem END CERTIFICATE RJ <	fqH1509jMcZ3uZrciC SkUAZqin/56HjuGb4h c38yo1P/I7UsueE3OR DZaOZ3k9Wo5QzUTPmd CQUESTsna	< × 1
Certificate Templ	late:		
	CC Web Server	~	_
Additional Attribu	utes:		_
Attributes:		a.	
		Submit >	_

步骤6.单击"提**交"**。

步骤7.选择Base 64编码,然后单击Download certificate,如图所示。

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

步骤8.保存文件并单击"确定"。文件保存在"下载"**文件**夹中。

步骤9.将文件重命名为finesse.cer。

导入Finesse应用和根签名证书

步骤1.在Web浏览器上,打开**Finesse OS Admin页**面,然后导航**至Security**> Certificate Management**。**

步骤2.单击Upload Certificate/Certificate chain按钮,如图所示。

Certificate List	Deload Certificate/Certificate chain	Generate CSR
Certificate List	0	-0
Find Certificate List whe	re Certificate 💽 begins with	
Generate Self-signed	Upload Certificate/Certificate ch/	ain Generate CSR

步骤3.在弹出窗口中,为Certificate Purse选择tomcat-trust作为证书用途。

步骤4.单击Browse...按钮并选择要导入的根证书文件。然后,单击"打开"按钮。

步骤5.在说明中写下类似tomcatrootcert的内容,然后单击Upload按钮,如图所示。

Upload Certificate/Certific	ate chain	
Dipload 🖳 Close		
Status Warning: Uploading a cl	uster-wide certificate will distribute it to all servers in this cluster]
Upload Certificate/Certifi Certificate Purpose* Description(friendly name) Upload File	tomcat-trust v tomcatrootcert Browse rootAll.cer]
Upload Close	em.	-
¢		>

步骤6.等到您看到Success(成功):Certificate Uploaded消息以关闭窗口。

系统将要求您重新启动系统,但首先,继续上传Finesse应用程序签名的证书,然后您可以重新启动 系统。

③ ♣ https://finessea.cc.lab:8443/cmplatform/certificateUpload.do		${\times}$	☆	≡
Upload Certificate/Certificate chain				
Dupload 🖳 Close				
Status Success: Certificate Uploaded Restart the node(s) using the CLI command, "utils system restart".				
Upload Certificate/Certificate chain				_
Certificate Purpose* tomcat-trust Description(friendly name)	-			
Upload File Browse No file selected.				
Upload Close i *- indicates required item.				
<				>

步骤7.单击Upload Certificate/Certificate chain按钮上的更多时间以导入Finesse应用程序证书。

Certificate List	
Generate Self-signed	Upload Certificate/Certificate chain
Certificate List	
Find Certificate List whe	re Certificate 💌 begins with 💌
Generate Self-signed	Upload Certificate/Certificate chain Generate CSR

步骤8.在弹出窗口中,选择Tomcat for Certificate Purse。

步骤9.单击Browse...**按钮,**然后选择Finesse CA签名文件**finesse.cer**。然后,单击"打**开"**按钮。

步骤10.单击"上传**"按**钮。

TD and the second	ote caom		
Upload Close			
tatus			
tatus			
Dura in the second	the state of the second st	to all the shares of	
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 cl Upload Certificate/Certifi Certificate Purpose*	cate chain	in this cluster	
Warning: Uploading a cl Upload Certificate/Certifi Certificate Purpose* Description(friendly name)	cate chain tomcat Self-signed certificate	in this cluster	

步骤11.等到您看到Success(成功):**证书上传**消息。

同样,系统要求您重新启动系统。关闭窗口并继续重新启动系统。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。