在CCE 12.6解决方案中实施CA签名证书

目录

简介 <u>先决条件</u> 要求 使用的组件 背景 步骤 基于CCE Windows的服务器 1.生成CSR 2.获取CA签名证书 3.上传CA签名证书 4.将CA签名的证书绑定到IIS 5.将CA签名的证书绑定到诊断门户 6.将根证书和中间证书导入Java密钥库 CVP解决方案 1.使用FQDN生成证书 <u>2.生成CSR</u> 3.获取CA签名证书 <u>4.导入CA签名</u>证书 <u>VOS服务器</u> 1.生成CSR证书 2.获取CA签名证书 3.上传应用和根证书 验证 故障排除 相关信息

简介

本文档介绍如何在Cisco Contact Center Enterprise(CCE)解决方案中实施证书颁发机构(CA)签名证书。

先决条件

要求

Cisco 建议您了解以下主题:

- 统一联络中心企业版(UCCE)版本12.6.2
- Package Contact Center Enterprise版本12.6.2

- 客户语音门户(CVP)版本12.6.2
- 思科虚拟化语音浏览器(VVB)
- 思科CVP操作和管理控制台(OAMP)
- 思科统一情报中心(CUIC)
- Cisco Unified Communications Manager (CUCM)

使用的组件

本文档中的信息基于以下软件版本:

- PCCE 12.6.2
- CVP 12.6.2
- 思科VVB 12.6.2
- Finess 12.6.2
- CUIC 12.6.2
- Windows 2019

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

证书用于确保客户端和服务器之间的身份验证通信安全。用户可以从CA购买证书,也可以使用自签 名证书。

自签名证书(顾名思义)由身份经过其认证的同一实体签名,而不是由证书颁发机构签名。自签名 证书并不像CA证书那样安全,但是在许多应用程序中默认使用自签名证书。

在Package Contact Center Enterprise(PCCE)解决方案版本12.x中,该解决方案的所有组件均由单一平台(SPOG)控制,该平台托管在主要管理工作站(AW)服务器中。

由于PCCE 12.5(1)版本中的安全管理合规性(SRC),SPOG和解决方案中的其他组件之间的所有通信 都通过安全的HTTP协议完成。

本文档详细介绍在CCE解决方案中实施CA签名证书以实现安全HTTP通信所需的步骤。有关任何其他UCCE安全注意事项,请参阅<u>UCCE安全指南</u>。

有关不同于安全HTTP的其他CVP安全通信,请参阅CVP配置指南:CVP安全指南<u>中的安全指南</u>。

注:本文档仅适用于CCE版本12.6。有关其他版本的链接,请参阅相关信息部分。

步骤

基于CCE Windows的服务器

1.生成CSR

此过程说明如何从Internet信息服务(IIS)管理器生成证书签名请求(CSR)。

步骤1:登录到Windows,然后选择控制面板>管理工具> Internet信息服务(IIS)管理器。

步骤 2在Connections窗格中,点击服务器名称。系统将显示Server Home窗格。



第3步:在IIS区域中,双击Server Certificates。



第4步:在"操作"窗格中,单击创建证书请求。

File View Help				
Connections Q []	Server Certifica Use this feature to request and m websites configured for SSL Filter 7 Name Case ICM Dispersetic Frames.	tes anage certificates that the lifeb se f Go - S Show All Group by: housed To PCCLANNA.PCCCRCDN.class.c.	ver can use with Electron by PCCEAWS.PCCERCE	Actives Import_ Constructed for an Repueb- Conglete Centricute Repueb- Create Domain Centricute. Create Self-Signed Centricute. Examine Extension Centricute.
	Cisco ICM SSL Certificate	PCCLANA.PCCDRCDN.cisco.c.	PCCEANA.PCCERCI	Renewed Certificate Help

第五步:在Request Certificate对话框中,执行以下操作:

在显示的字段中指定所需信息,然后单击Next。

Request Certificate		?	x
Distinguished Na	me Properties		
Specify the required information official names and they cannot	n for the certificate. State/province and City/locality must be specified as contain abbreviations.		
Common name:	pcceawa.pccercdn.cisco.com		
Organization:	Cisco		
Organizational unit:	CX		
City/locality	RCDN		
State/province:	TX		
Country/region:	US v		
	Previous Next Finish	Cancel	

在Cryptographic service provider下拉列表中,保留默认设置。

从Bit length下拉列表中选择2048。

Request Certificate	7	x
Cryptographic Service Provider Properties		
Select a cryptographic service provider and a bit length. The bit length of the encryption key determines certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater length may decrease performance. Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider	the bit	
2048		
Previous Next Finish	Cance	
Previous Next Finish	Cancel	1

第六步:为证书请求指定文件名,然后单击Finish。

Request Certificate	?	x
File Name		
Specify the file name for the certificate request. This information can be sent to a certification authority fo signing.	w	
PCCEAW.PCCERCDN.cisco.com		
Previous Next Finish	Cancel	

2.获取CA签名证书

步骤1:在CA上签署证书。

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。

第二步:从证书颁发机构(根、应用和中级,如果有)获取CA签名证书。

3.上传CA签名证书

步骤1:登录到Windows,然后选择控制面板>管理工具> Internet信息服务(IIS)管理器。



步骤 2在Connections窗格中,点击服务器名称。

File View Help							
Connections 오, • 급 솔 용.	Sala PC	CEAWA H	ome				
Start Page	Filter		• ¥ 60 - 1	Show All	Group by:		
	Connection	Chattle Lamai					٨
	Strings IIS						
	2	2	0	1	4	2	
	Authentic	Compression	Default Document	Directory Browsing	Error Pages	Handler Mappings	
		e	5	4		- P	
	HTTP Redirect	HTTP Respon	ISAPI and CGI Restri	ISAPI Filters	Logging	MME Types	•
	4	1	8		2		
	Modules	Output Caching	Request Filtering	Server Certificates	Worker Processes		
	Manageme	HL.	_			*	
	Conference		1				
	Consignation.	A ADDRESS A	10.000				

第3步:在IIS区域中,双击服务器证书。



第4步:在Actions窗格中,点击Complete Certificate Request。

File View Help				
Connections Q. • [2] = [9] V Start Page PCCEARIA (PCCERCON proceedmin)	Server Certificates Use this feature to request and manage certificates that the lifeb server can use with websites configured for SSL.			Actions Import Create Certificate Request Complete Certificate Request
	Filter 7	Go - C Show All Group by: Issued To	R. Issued By	Create Domain Cettificate Create Self-Signed Cettificate
	Cisca ICM Diagnostic Framew Cisca ICM 325 Cettificate	PCOLINA.PCORDN.cisci PCOLINA.PCORDN.cisci	PCCEANIA.PCCERCI PCCEANIA.PCCERCI	Enable Automatic Rabind of Renewed Cotificate Help

第5步:在Complete Certificate Request对话框中,填写以下字段:

在包含证书颁发机构响应字段的文件名中,点击……按钮。

浏览到已签名应用证书的存储位置,然后点击Open。

注:如果这是二层CA实施,并且根证书尚未在服务器证书存储中,则需要在导入签名证书之 前将根证书上传到Windows存储中。如果需要将根CA上传到Windows应用商店<u>Microsoft</u>— <u>安装受信任的根证书</u>,请参阅本文档。

在"友好名称"字段中,输入服务器的完全限定域名(FQDN)或任何重要名称。确保Select a certificate store for the new certificate下拉列表保留为Personal。

Complete Certificate Request	?	×
Specify Certificate Authority Response		
Complete a previously created certificate request by retrieving the file that contains the certificate authori response.	ty's	
File name containing the certification authority's response: C:\Certificates\PCCEAWcertnew.cer		
Friendly name: PCCEAWA.pccercdn.cisco.com		
Select a certificate store for the new certificates		
Personal v		
ОК	Cancel	

步骤 6 单击OK上传证书。

如果证书上传成功,则证书将显示在Server Certificates窗格中。

bitemet Information Services (IS) Manager			-	۰	×
				- 8	•
File View Help					
Connections	Canada Cartificator	Actions			
Q. El 12 19.	Server certificates	Import	-		
Stat Page N PCCLANA (PCCIRCDN pcceadmin)	Use this feature to request and manage certificates that the Web server can use with websites configured for VL.	Create	Centro	ne Reque	- 10
	Day . W.G D. Day M. Kennelse	Compo	na can	Catilica	and a second second
	New Manual Institution	Creater		and Card	fante.
	Cisco ICM Diagnostic Framework servi. PCCLAHA.PCCDRCDN.cisco.c. PCCLAHA.P	Enable.	laters.	etic Rabie	al ef
	Cece ICM SR. Cetificate PCCEARA.PCCBCDN.cece.c. PCCEARA.P	Renew	ed Certi	licate	
	PCCEARA.pccercdit.clsco.com proseesa.pccercdit.clsco.com PCCERCDIV-	🚱 Help			

4.将CA签名的证书绑定到IIS

此过程说明如何在IIS管理器中绑定CA签名证书。

步骤1:登录到Windows,然后选择控制面板>管理工具> Internet信息服务(IIS)管理器。



步骤 2在Connections窗格中,选择<server_name> > Sites > Default Web Site。



第3步:在"操作"窗格中,单击"绑定……"



第4步:单击带有端口443的https类型,然后单击Edit...。

File View Help					
Connections		Conformate 14 feet	City Harris		Actions
9,- 🔛 🙇 👂. 👘		Default Wet	Site Home		2 Explore
Start Page	Ste lindings			7 X	Edit Permissions
- PECEARA (PECERCOMpose		a la company			Edit Site
544	type root name	Pot PASSIES	anong mome.	Add_	Bindings
> 😝 Default Hieb Site	inter .	40		Edt.	Basic Settings
					View Applications
				Remove	View Virtual Directories
				Beness	Manage Website 🛞
				·	2 Restart
					F Stat.
					· Stop
					Browse Website
					Browse 180 (Http)
					CE Browse (4G (Https)
					Advanced Settings
					Configure
				Occe	Carally
					0 Help
		🔹 😭	0		
			Contractor of the Contractor o	-	
		ovjot rejutil	are beginds		
		🔀 Features View 🛃 Center	Wew		
B-1.1					

第5步:从SSL证书(SSL certificate)下拉列表中,选择与上一步中给定的友好名称相同的证书。

Ny Internet Information Services (IS) Manager	- 0 X
General PCCEANA + Ses + Debuilt Web Ses +	0 H 🗄 1 😣 •
File View Help	
Connections Default Week Site Horne	Actions
Q. El A IS.	🛓 Depiere
Statistics	Lot Permissions
Application Pools Type Host Name Post IP Address Binding Informa. Appl.	Ldt Ste
V 2 Ster	Test Series
) @ Debut web 584	Yes Applications
Renove	Vew Virtual Directories
Edit Site Binding	Manage Website 🛞
Tope Paddess Parts	2 feater
https://www.international.com	Estat
Hod name	· 300
	Fromse Website
Require Server Name Indication	E Browse (443 (https)
	Advanced Settings
Ett undfaste	Configure
PCCLARKA accords circa com	Umb.
	8 Hep
27 Card	
To Features View Content View	
Ready	۹.

步骤 6 Click OK.

步骤 7.导航到开始>运行> services.msc,然后重新启动IIS管理服务。



5.将CA签名的证书绑定到诊断门户

此过程说明如何在Diagnostic Portico中绑定CA签名证书。

步骤1:打开命令提示符(以管理员身份运行)。

步骤 2导航到Diagnostic Portico主文件夹。运行此指令:

第3步:删除当前绑定到Diagnostic Portico的证书。运行此指令:

DiagFwCertMgr /task:UnbindCert

c:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:UnbindCert
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
Executing Task: 'UnbindCert'
Read port number from service configuration file: '7890'
ATTEMPTING TO UNBIND CERTIFICATE FROM WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Attempting to delete the existing binding on 0.0.0.0:7890
Deleted existing binding successfully
Deleted entry from the service registry
ALL TASKS FOR UNBINDING THE CERTIFICATE FROM HTTP SERVICE COMPLETED SUCCESSFULLY

c:\icm\serviceability\diagnostics\bin>

第4步:打开签名证书并复制Thumbprint字段的哈希内容(不含空格)。

注意:确保从散列内容的开头或结尾删除任何隐藏字符。像记事本++这样的编辑器可以帮助 您识别这些隐藏字符。

Certificate	×
General Details Certification Path	
Show: <all></all>	
Field Value /	1
CRL Distribution Points [1]CRL Distribution Point: Distr	
Authority Information Access [1]Authority Info Access: Acc Certificate Template Inform Template=CC Web Server(1.3	
Application Policies [1]Application Certificate Polic	
Thumbprint algorithm sha1 Thumbprint 97 93 74 00 99 19 53 d6 4e 0b	
97 93 74 00 99 19 53 d6 4e 0b c5 6e c4 4c bd 96 36 dc 4b cb	
	1
Edit Properties Copy to File	1
	_
OK	

第五步:运行此命令并粘贴哈希内容。

::\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:BindCertFromStore /certhash:97937400991953d64e0bc56ec44cbd963 ic4bcb

Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager Executing Task: 'BindCertFromStore' Read port number from service configuration file: '7890' CertHash Argument Passed: '97937400991953d64e0bc56ec44cbd9636dc4bcb' ATTEMPTING TO BIND CERTIFICATE WITH WINDOWS HTTP SERVICE Binding IP Address: '0.0.0.0:7890' Trying to look up certificate: 97937400991953D64E0BC56EC44CBD9636DC4BCB Local Computer Personal certificate store was opened successfully Certificate requested found in store Certificate store was closed successfully Certificate bind with HTTP service on 0.0.0:7890 completed successfully Found existing registry key for the service Hash of certificate used sawed in the service registry ALL TASKS FOR BINDING THE CERTIFICATE WITH HTTP SERVICE COMPLETED SUCCESSFULLY

:\icm\serviceability\diagnostics\bin>

如果证书绑定成功,则会显示证书绑定为VALID消息。

第六步:验证证书绑定是否成功。运行此指令:

DiagFwCertMgr /task:ValidateCertBinding

::\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:ValidateCertBinding Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager Executing Task: 'ValidateCertBinding' Read port number from service configuration file: '7890' ATTEMPTING TO VALIDATE CERTIFICATE BINDING WITH WINDOWS HTTP SERVICE Binding IP Address: '0.0.0.0:7890' Attempting to query HTTP service for SSL certificate binding Found a certificate binding on 0.0.0.0:7890 Attempting to locate this certificate in the Local Computer certificate store Trying to look up certificate: 97937400991953D64E0BC56EC44CBD9636DC4BCB Local Computer Personal certificate store was opened successfully Certificate requested found in store Certificate store was closed successfully The certificate binding is VALID <u>Certificate hash stored in service registry matches certificate used</u> by service ALL TASKS FOR VALIDATING CERTIFICATE BINDING COMPLETED SUCCESSFULLY

c:\icm\serviceability\diagnostics\bin>_

注意:默认情况下,DiagFwCertMgr使用端口7890。

如果证书绑定成功,则会显示证书绑定为VALID消息。

步骤 7.重新启动诊断框架服务。运行以下命令:

net stop DiagFwSvc
net start DiagFwSvc

如果诊断框架成功重新启动,则启动应用程序时不会显示证书错误警告。

6.将根证书和中间证书导入Java密钥库

注意:在开始之前,您必须备份密钥库并以管理员身份从Java主目录运行命令。

步骤1.了解Java主路径以确保承载Java密钥工具的位置。可通过几种方法查找java home路径。

选项1: CLI命令: echo %CCE_JAVA_HOME%



选项2:通过高级系统设置手动设置,如图所示

v 🛧 🔽 v Control Pan	al & Sustem and Security & Sustem			Search Control Panel
	er > System and security > System		•0	Search Control Panel
ol Panel Home	System Properties ×]		
e Manager	Computer Name Hardware Advanced Remote	Environment Variables		
nced system settings	You must be logged on as an Administrator to make most of these changes. Performance			
	Visual effects, processor scheduling, memory usage, and virtual memory	User variables for Administrator		
	C.W.o.s	Variable	Value	
	Settings	Path TEMP	C:\Users\Administrator\AppData\Local\Microsoft\WindowsAp C:\Users\Administrator\AppData\Local\Temp	pps;
	User Profiles	TMP	C:\Users\Administrator\AppData\Local\Temp	
	Desktop settings related to your sign-in Settings	*		
	Startup and Recovery			
	System startup, system failure, and debugging information		New	Edit Delete
	Settings	System variables		
	Environment Variables	Variable	Value	
	Environment valiables	CCE_JAVA_HOME	C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot	
		COMPLUS_ProtAPI_ProfilerC	C:\Windows\system32\cmd.exe	
	OK Cancel Apply	COR_ENABLE_PROFILING	1	
		COR_PROFILER	AppDynamics.AgentProfiler	
		CORECLR_ENABLE_PROFILI	I AppDynamics.AgentProfiler	
			New	Edit Delete
			New	Delete
			-	OV Canad
			L	Cancel
so				

%CCE_JAVA_HOME%\lib\security\cacerts备份cacerts文件。 您可以将其复制到其他位置。

第三步:以管理员身份打开命令窗口,然后运行以下命令:

cd %CCE_JAVA_HOME%\bin

keytool.exe -keystore <ICM install directory>\ssl\cacerts -trustcacerts -import -file <path where the R
keytool.exe -keystore %CCE_JAVA_HOME%\lib\security\cacerts -trustcacerts -import -file <path where the</pre>

注:所需的特定证书取决于您用于签署证书的CA。在双层CA中(这是公共CA的典型形式 ,比内部CA更安全),您需要导入根证书和中间证书。在没有中间体的独立CA中(通常在实 验室或更简单的内部CA中可见),您只需要导入根证书。根证书和中间证书必须导入ICM和 OpenJDK密钥库,因为System CLI仍使用OpenJDK密钥库。

CVP解决方案

1.使用FQDN生成证书

此过程说明如何使用FQDN为Web服务管理器(WSM)、语音XML(VXML)、呼叫服务器和操作管理 (OAMP)服务生成证书。

注意:安装CVP时,证书名称仅包含服务器的名称,而不包含FQDN,因此,您需要重新生成 证书。

注意:开始之前,必须执行以下操作: 1.以管理员身份打开命令窗口。 2.对于12.6.2,要标识密钥库密码,请转到%CVP_HOME%\bin文件夹并运行 DecryptKeystoreUtil.bat文件。 3.对于12.6.1,要识别密钥库密码,请运行命令,more %CVP_HOME%\conf\security.properties。 4.运行keytool命令时需要此密码。 5.从%CVP HOME%\conf\security\目录运行命令copy_keystore backup.keystore。

CVP服务器

步骤1:要删除CVP服务器证书,请运行以下命令:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a 出现提示时,输入密钥库密码。

第二步:要生成WSM证书,请运行以下命令:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai

出现提示时,输入密钥库密码。

注:默认情况下,证书生成时间为两年。使用 — validity XXXX设置重新生成证书时的到期日 期,否则证书有效期为90天,并且需要在此时间之前由CA签名。对于大多数此类证书,3-5年 必须是合理的验证时间。

以下是一些标准有效性输入:

一年	365
两年	730
三年	1095
四年	1460
五年	1895
十年	3650

注意:从12.5证书必须是SHA 256、密钥大小2048和加密算法RSA,请使用以下参数设置以 下值:-keyalg RSA和 — keysize 2048。CVP密钥库命令必须包括 — storetype JCEKS参数 。如果不这样做,证书、密钥或更糟的密钥库可能会损坏。

在问题中指定服务器的FQDN,您的名字和姓是什么?

C:\Cisco\CVP\jre\bin>keytool.exe -genkeypair -v -storetype JCEKS -keystore c:\Cisco\CVP\conf\security\.keystore -ali sm_certificate1 -keysize 2048 -keyalg RSA Enter keystore password: What is your first and last name? [Unknown]: cvp.bora.com What is the name of your organizational unit? [Unknown]:

完成以下其他问题:

您的组织单位名称是什么?

[未知]:<指定OU>

贵公司的名称是什么?

[未知]:<指定组织的名称>

您的城市或地区名称是什么?

[未知]:<指定城市/地区的名称>

您所在省/自治区/直辖市的名称是什么?

[未知]:<指定州/省的名称>

此设备的国家代码是多少(两个字母)?

[未知]:<指定两个字母的国家/地区代码>

为接下来的两个输入指定yes。

第三步:对vxml_certificate和callserver_certificate执行相同的步骤:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai

CVP报告服务器

步骤1:要删除WSM和报告服务器证书,请运行以下命令:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a

出现提示时,输入密钥库密码。

第二步:要生成WSM证书,请运行以下命令:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai

出现提示时,输入密钥库密码。

指定用于查询的服务器FQDN您的姓和名是什么?并继续执行与CVP服务器相同的步骤。

第三步:对callserver_certificate执行相同的步骤:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai

出现提示时,输入密钥库密码。

CVP OAMP(UCCE部署)

由于在PCCE解决方案版本12.x中,该解决方案的所有组件都由SPOG控制,并且未安装OAMP,因此仅对于UCCE部署解决方案而言,才需要这些步骤。

步骤1:要删除WSM和OAMP服务器证书,请运行以下命令:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a

出现提示时,输入密钥库密码。

第二步:要生成WSM证书,请运行以下命令:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai

出现提示时,输入密钥库密码。

指定用于查询的服务器FQDN您的姓和名是什么?并继续执行与CVP服务器相同的步骤。

第三步:对oamp_certificate执行相同的步骤:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai

出现提示时,输入密钥库密码。

2.生成CSR

注意:符合RFC5280标准的浏览器要求每个证书中都包含主题备用名称(SAN)。在生成 CSR时,可以在SAN中使用 — ext参数完成此操作。

主题备用名称

-ext参数允许用户使用特定分机。显示的示例添加了主题备用名称(SAN),该名称带有服务器的完全 限定域名(FQDN)以及本地主机。其他SAN字段可作为逗号分隔值添加。

有效的SAN类型包括:

ip:192.168.0.1
dns:myserver.mydomain.com
email:name@mydomain.com

例如:

-ext san=dns:mycvp.mydomain.com,dns:localhost

CVP服务器

步骤1:生成别名的证书请求。运行此命令并将其保存到文件(例如,wsm_certificate):

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -

出现提示时,输入密钥库密码。

'第二步:对vxml_certificate和callserver_certificate执行相同的步骤:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -

出现提示时,输入密钥库密码。

CVP报告服务器

步骤1:生成别名的证书请求。运行此命令并将其保存到文件(例如,wsmreport_certificate):

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -

出现提示时,输入密钥库密码。

第二步:对callserver_certificate执行相同的步骤:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -

出现提示时,输入密钥库密码。

CVP OAMP(仅限UCCE部署)

步骤1:生成别名的证书请求。运行此命令并将其保存到文件(例如,wsmoamp_certificate):

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -

出现提示时,输入密钥库密码。

第二步:对oamp_certificate执行相同的步骤:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -

出现提示时,输入密钥库密码。

3.获取CA签名证书

步骤1:在CA上签署证书(CVP服务器的WSM、Callserver和VXML服务器;CVP OAMP服务器的 WSM和OAMP,CVP报告服务器的WSM和Callserver)。

第二步:从CA机构下载应用证书和根证书。

第三步:将根证书和CA签名证书复制到每台服务器的%CVP_HOME%\conf\security\文件夹中。

4.导入CA签名证书

将这些步骤应用于CVP解决方案的所有服务器。 仅需要导入该服务器上组件的证书CA签名证书。 步骤1:导入根证书。运行此指令: %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t

出现提示时,输入密钥库密码。在Trust this certificate提示符下,键入Yes。 如果存在中间证书,请运行以下命令:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t

出现提示时,输入密钥库密码。在Trust this certificate提示符下,键入Yes。 第二步:为该服务器证书(CVP、Reporting和OAMP)导入CA签名WSM。运行此指令:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t

出现提示时,输入密钥库密码。在Trust this certificate提示符下,键入Yes。

第三步:在CVP服务器和报告服务器中导入Callserver CA签名证书。运行此指令:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t

出现提示时,输入密钥库密码。在Trust this certificate提示符下,键入Yes。 第四步:在CVP服务器中导入VXML服务器CA签名证书。运行此指令:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t

出现提示时,输入密钥库密码。在Trust this certificate提示符下,键入Yes。 第五步:在CVP OAMP服务器(仅适用于UCCE)中导入OAMP服务器CA签名证书。运行此指令:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -t

出现提示时,输入密钥库密码。在Trust this certificate提示符下,键入Yes。

第六步:重新启动服务器。

注意:在UCCE部署中,请确保使用生成CSR时提供的FQDN在CVP OAMP中添加服务器 (CVP报告、CVP服务器等)。

VOS服务器

1.生成CSR证书

此程序说明如何从基于思科语音操作系统(VOS)的平台生成Tomcat CSR证书。

此过程适用于基于VOS的应用,例如:

- Finesse
- CUIC \实时数据(LD)\身份服务器(IDS)
- 云连接
- 思科VVB

步骤1:导航至Cisco Unified Communications Operating System Administration页面 : https://FQDN :<8443或443>/cmplatform。

第二步:导航到安全>证书管理,然后选择生成CSR。

Show - Settings - Se	curty - Software Upgrades -	Services - Help -	
Certificate List			
Quererate Self-signed	Colored Certificate/Certificate	chain 💽 Generate CSR	
Certificate List			
Find Certificate List whe	e Certificate · begins	with ~	Find Clear Filter 💠 🚥
		No a	tive query. Please enter your search criteria using the options above.
Generate Self-signed	Upload Certificate/Certifica	te chain Generate CSR	

第三步:生成CSR证书后,关闭窗口并选择下载CSR。

Show . Settings . Security . Software Upgrades . Services . Help .
Certificate List
😨 Generate Self-signed in Upload Certificate/Certificate chain 👔 Generate CSR
Certificate List
Find Certificate List where Certificate 🗸 begins with 🗸 Find Clear Filter 🔯 🚥
No active query. Please enter your search oriteria using the options above.
Generate Self-signed Upload Certificate/Certificate chain Generate CSR Download CSR

第四步:确保证书目的为tomcat,然后单击Download CSR。

i Download Certificate Signing Request - Mozilla Firefox	-		×
🛛 🖗 https://10.201.224.234/cmplatform/certificateDownloadNewCsr.do		•••	≡
Download Certificate Signing Request			
Download CSR 🖳 Close			
Status Certificate names not listed below do not have a corresponding CSR Download Certificate Signing Request Certificate Purpose* tomcat Download CSR Close ··································			
<			>

第五步:单击Save File。文件保存在Download文件夹中。



2.获取CA签名证书

步骤1:在CA上导出的tomcat证书上签名。

第二步:下载应用和从CA机构认证的根证书。

3.上传应用和根证书

步骤1:导航至Cisco Unified Communications Operating System Administration页面 : <u>https://FQDN</u>:<8443或443>/cmplatform。

第二步:导航到安全>证书管理,然后选择上传证书/证书链。



第三步:在Upload certificate/Certificate chain窗口中,选择tomcat-trust in certificate purpose字段 并上传根证书。

Upload Certificate/Certificate chain			
Upload 🖳 Close			
Status Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster			
Upload Certificate/Certificate chain			
Certificate Purpose*	tomcat-trust		
Description(friendly name)			
Upload File	Choose File No file chosen		
Upload Close			

第四步:将中间证书(如果有)作为tomcat-trust上传。

第五步:在Upload certificate/Certificate chain(上传证书/证书链)窗口中,选择Certificate Purpose(证书用途)字段中的now tomcat,然后上传应用CA签名的证书。

Upload Certificate/Certificat	te chain	
Dipload 🖳 Close		
Status Warning: Uploading a clus	ter-wide certificate will distribute it to all servers in this cluster]
Certificate Purpose*	tomcat	
Description(friendly name)	Self-signed certificate	
Upload File	Browse No file selected.	
Upload Close	n.	
<		\geq

第六步:重新启动服务器。

验证

重新启动服务器后,请执行以下步骤以验证CA签名的实现:

步骤1:打开Web浏览器并清除缓存。

第二步:关闭,然后再次打开浏览器。

现在,您必须看到证书开关以开始CA签名的证书,并且浏览器窗口中指示证书是自签名的,因此不 受信任,必须离开。

故障排除

本指南中没有用于排除CA签名证书实施故障的步骤。

相关信息

- <u>CVP配置指南 安全</u>
- <u>UCCE安全指南</u>
- PCCE管理指南
- <u>交换PCCE自签名证书 PCCE 12.5</u>

- Exchange UCCE自签名证书 UCCE 12.5
- <u>交换PCCE自签名证书 PCCE 12.6</u>
- Exchange UCCE自签名证书 UCCE 12.6
- <u>证书交换实用程序</u>
- <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)。

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)。