# PCCE解决方案中的Exchange自签名证书

## 目录

简介 先决条件 要求 使用的组件 背景 步骤 <u>第1部分:CVP和ADS服务器之间的证书交换</u> 步骤1.导出CVP服务器证书 步骤2.将CVP服务器WSM证书导入ADS服务器 步骤3.导出ADS服务器证书 步骤4.将ADS服务器导入CVP服务器和报告服务器 第2部分:VOS平台应用与ADS服务器之间的证书交换 步骤1.导出VOS平台应用服务器证书。 步骤2.将VOS平台应用导入ADS服务器 第3部分:Roggers、PG和ADS服务器之间的证书交换 步骤1.从Rogger和PG服务器导出IIS证书 步骤2.从Rogger和PG服务器导出诊断框架门户(DFP)证书 步骤3.将证书导入ADS服务器 第4部分: CVP CallStudio WEBService集成 相关信息

## 简介

本文档介绍如何在Cisco Packaged Contact Center Enterprise(PCCE)解决方案中的主管理服务器 (ADS/AW)和其他应用服务器之间交换自签名证书。

作者:Anuj Bhatia、Robert Rogier和Ramiro Amaya,思科TAC工程师。

## 先决条件

## 要求

Cisco 建议您了解以下主题:

- PCCE版本12.5(1)
- •客户语音门户(CVP)版本12.5(1)

## 使用的组件

本文档中的信息基于以下软件版本:

• PCCE 12.5(1)

• CVP 12.5(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

在12.x的PCCE解决方案中,所有设备都通过托管在主AW服务器中的单一玻璃板(SPOG)进行控制 。由于PCCE 12.5(1)版本中的安全管理合规性(SRC),因此SPOG与解决方案中其他服务器之间的 所有通信都严格通过安全HTTP协议完成。

证书用于实现SPOG与其他设备之间的无缝安全通信。在自签名证书环境中,服务器之间的证书交换成为必须。此证书交换对于启用12.5(1)版本中的新功能(如智能许可、Webex体验管理(WXM)和 客户虚拟助理(CVA))也是必需的。

### 步骤

这些是自签名证书的导出组件和自签名证书需要导入的组件。

(i) 主AW 服务器:此服务器需要证书来自:

- Windows平台: ICM: 路由器和记录器(Rogger){A/B}、外围网关(PG){A/B}、所有ADS和电子邮件与聊天(ECE)服务器。 注意:需要IIS和诊断框架证书。CVP:CVP服务器、CVP报告服务器。
   注释 1:需要来自服务器的Web服务管理(WSM)证书。注释 2:证书必须具有完全限定域名(FQDN)。
- VOS平台:云连接、思科虚拟语音浏览器(VVB)、思科统一呼叫管理器(CUCM)、Finesse、思 科统一智能中心(CUIC)、实时数据(LD)、身份服务器(IDS)和其他适用服务器。

解决方案中的其他ADS服务器也是如此。

(ii)路由器\记录器服务器:此服务器需要证书来自:

• Windows平台: 所有ADS服务器IIS证书。 (iii)CUCM PG服务器:此服务器需要证书来自:

• VOS平台:CUCM发布者。 注意:从CUCM服务器下载JTAPI客户端时需要执行此操作。 (iv)CVP服务器:此服务器需要来自

• Windows平台: 所有ADS服务器IIS证书

• VOS平台:用于WXM集成的云连接服务器,用于安全SIP和HTTP通信的VVB服务器。 (v)CVP报告服务器:此服务器需要证书来自:

• Windows平台: 所有ADS服务器IIS证书 (vi)VVB**服务器:**此服务器需要证书来自:

•Windows平台:CVP VXML服务器(安全HTTP)、CVP呼叫服务器(安全SIP) 在解决方案中有效交换自签名证书所需的步骤分为三个部分。

第1部分:CVP服务器和ADS服务器之间的证书交换。

第2部分:VOS平台应用和ADS服务器之间的证书交换。

第3部分:Roggers、PG和ADS服务器之间的证书交换。

#### 第1部分:CVP和ADS服务器之间的证书交换

成功完成此交换所需的步骤如下:

步骤1.导出CVP服务器WSM证书。

步骤2.将CVP服务器WSM证书导入ADS服务器。

步骤3.导出ADS服务器证书。

步骤4.将ADS服务器导入CVP服务器和CVP报告服务器。

#### 步骤1.导出CVP服务器证书

在从CVP服务器导出证书之前,您需要使用服务器的FQDN重新生成证书,否则,像智能许可、 CVA和CVP与SPOG同步这样的一些功能可能会遇到问题。

**警告:**在开始之前,您必须执行以下操作:

- 获取密钥库密码。运行此指令: 更多%CVP\_HOME%\conf\security.properties
- 将%CVP\_HOME%\conf\security文件夹复制到另一个文件夹。
- •以管理员身份打开命令窗口以运行命令。

**注意:**您可以使用keytool参数 — storepass简化本文档中使用的命令。对于所有CVP服务器 ,粘贴从指定的security.properties文件获取的密码。对于ADS服务器,键入密码:**常见** 

要在CVP服务器上重新生成证书,请执行以下步骤:

#### (i)列出服务器中的证书

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore list

**注意:**CVP服务器具有以下自签名证书:wsm\_certificate 、 vxml\_certificate 、 callserver\_certificate。如果使用keytool的参数 — v,则可以查看每个证书的更多详细信息。 此外,还可以在keytool.exe list命令的末尾添加">"符号,以将输出发送到文本文件,例如: > test.txt

#### (ii)删除旧的自签证书

CVP服务器:用于删除自签名证书的命令:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore delete -alias vxml\_certificate

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore delete -alias callserver\_certificate

#### CVP报告服务器:用于删除自签名证书的命令:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore delete -alias wsm\_certificate

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore delete -alias callserver\_certificate

#### 注意:CVP报告服务器具有这些自签名证书wsm\_certificate、callserver\_certificate。

#### (iii)使用服务器的FQDN生成新的自签名证书

#### CVP服务器

为WSM生成自签名证书的命令:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore genkeypair -alias wsm\_certificate -keysize 2048 -keyalg RSA -validity XXXX 在问您的姓和名是什么时,指定服务器的FQDN?



完成以下其他问题:

您的组织单位的名称是什么?

[未知]:<指定OU>

*贵组织的名称是什么?* 

[未知]:<指定组织的名称>

您所在城市或地区的名称是什么?

[未知]:<指定城市/地区名称>

您所在州或省的名称是什么?

[未知]:<指定省/自治区名称>

此设备的双字母国家/地区代码是什么?

#### [未知]:<指定双字母国家/地区代码>

#### 为接下来的两个输入指定yes。

#### 对vxml\_certificate和callserver\_certificate执行相同步骤:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore genkeypair -alias vxml\_certificate -keysize 2048 -keyalg RSA -validity XXXX

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore genkeypair -alias callserver\_certificate -keysize 2048 -keyalg RSA -validity XXXX

#### 重新启动CVP呼叫服务器。

#### CVP报告服务器

为WSM生成自签名证书的命令:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore genkeypair -alias wsm\_certificate -keysize 2048 -keyalg RSA -validity XXXX 为查询指定服务器的FQDN,您的姓和名是什么?并遵循与CVP服务器相同的步骤。

#### 对callserver\_certificate执行相同的步骤:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore genkeypair -alias callserver\_certificate -keysize 2048 -keyalg RSA -validity XXXX

#### 重新启动报告服务器。

**注意:**默认情况下,自签名证书生成两年。使用 — validity XXXX设置重新生成证书时的到期 日期,否则证书的有效期为90天。对于这些证书中的大多数,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

警告:在12.5中,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。如果不执行此操作,证书、密钥或更糟的密钥库可能会损坏。

#### (iv)从CVP和报告服务器导出wsm\_Certificate

a)将WSM证书从每个CVP服务器导出到临时位置,并使用所需名称重命名证书。可将其重命名为

wsmcsX.crt。用唯一的数字或字母替换"X"。即wsmcsa.crt、wsmcsb.crt。

#### 用于导出自签名证书的命令:

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore export -alias wsm\_certificate -file %CVP\_HOME%\conf\security\wsm.crt

b)从路径C:\Cisco\CVP\conf\security\wsm.crt复制证**书**,*将*其重命名**为wsmcsX.crt**,并将其移动到 ADS服务器上的临时文件夹。

#### 步骤2.将CVP服务器WSM证书导入ADS服务器

要在ADS服务器中导入证书,您需要使用java工具集的一部分keytool。有几种方法可以找到此工具 托管的java主目录路径。

(i)CLI命令>回应%JAVA\_HOME%



(ii)通过高级**系统设置手**动进行,如图所示。

4> -> 🕆 🕈 🔜 Control	Panel + System and Security + System	v 0 Search	Control Panel	<i>р</i>
Control Panel Home	System Properties	×	1	• •
<ul> <li>Device Manager</li> <li>Romote settings</li> <li>Advanced system settings</li> </ul>	Computer Name Hardware Advanced Raw You must be logged on as an Administrator to	ute nake not d'these charges.	S - User variables for	n Administrator
	Vasal effects, processor scheduling, memory User holles Dedice settings related to your sprue.	usege, and vetual memory Settings	Variable Path TEMP TMP	Valve SubSERRORUEN-AppOntation SubSERRORUEN-AppOntation SubSERRORUEN-AppOntation
	Statup and Recovery System statup, system falues, and debuggin	Setings	be	Ne
la de	OK	Setings Environment Vantables Cancel Avoly	System variables Variable Mon. Hotwo Mon. Hotwo NUMBER_OF_PI	Value C/Windowskystem32 and C/JProgram Files (460/Java) Observice provider standards ROCISSOFS 6
Security and Maintenance			Puth So to	Settings to a Cover are SAT CMD very with

#### 在PCCE 12.5上,默认路径为C:\Program文件(x86)\Java\jre1.8.0\_221\bin

#### 导入自签名证书的命令:

keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0\_221\lib\security\cacerts" -import storepass changeit -alias {fqdn\_of\_cvp} -file c:\temp\certs\wsmcsX.crt

#### 注意:对部署中的每个CVP重复这些命令,并在其他ADS服务器上执行相同任务

d)在ADS服务器上重新启动Apache Tomcat服务。

#### 步骤3.导出ADS服务器证书

对于CVP报告服务器,您必须导出ADS证书并将其导入报告服务器。以下是步骤:

(i)在浏览器的ADS服务器上,导航至服务器url:https://{servername}

(ii)将证书保存到临时文件夹,例如:c:\temp\certs并将证书命名为ADS{svr}[ab].cer

#### CCE via Chrome Browser

Certificate		×		
neral Details Certification Pa	n	th	E <sup>2</sup> Centificate Export Wand	
Neid	Value ^	4	Export File Format Certificates can be exported in a variety of file formats.	
Senat number Signature algorithm Signature hash algorithm Sasuer Yalid from Yalid fo	00 s9 ab 59 50 74 60 76 87 sha258554 aha256 am 125a.bora.com Mendey, September 30, 20 29 Sunday, September 25, 20 79 am 175a.bora.com	04	Select the format you want to use: DER encoded binary X.509 (.CER) Bisse 64 encoded X.509 (.CER) Chystographic Message Syntax Standard - PKCS #7 Certificates (.P78) Shuke all certificates in the certification path if possible Personal Information Exchange - INICS #12 (.P73) Shuke all certificates in the certification path if possible	
	Edit Properties		Depart of private way in the capacity is accusated     Depart of entended properties     Datable certificate privacy     Monsech Serviced Certificate Store (.557)	

注意:选择选项Base-64 encoded X.509(.CER)。

#### 步骤4.将ADS服务器导入CVP服务器和报告服务器

(i)将证书复制到C:\Cisco\CVP\conf\security目录中的CVP服务器和CVP报告服务器。

(ii)将证书导入CVP服务器和CVP报告服务器。

%CVP\_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP\_HOME%\conf\security\.keystore import -trustcacerts -alias {fqdn\_of\_ads} -file %CVP\_HOME%\conf\security\ICM{svr}[ab].cer 对其他ADS服务器执行相同步骤。

(iii)重新启动CVP服务器和报告服务器

### 第2部分:VOS平台应用与ADS服务器之间的证书交换

成功完成此交换所需的步骤如下:

步骤1.导出VOS平台应用服务器证书。

步骤2.将VOS平台应用证书导入ADS服务器。

此流程适用于所有VOS应用,例如:

- CUCM
- VVB
- Finesse
- CUIC \ LD \ IDS
- 云连接

步骤1.导出VOS平台应用服务器证书。

(i)导航至"思科统一通信操作系统管理"页:<u>https://FQDN:8443/cmplatform</u>

(ii)导航至Security > Certificate Management**,然后在Tomcat-trust文**件夹中查找应用程序主服**务器 证书**。

dealer. Cisco Unified Operating System Admin For Cace Unified Communications Information	vistrat	ion		Nevigation Class Unified 05 Administration • G administration About Login
Drov - Settings - Security - Schwarzuppieres - Secures - Halp -				
Gertificate List				
💫 bereite betrepet 🐴 spiset betrebetrebetre over 🖳 bereite	094			
toreshitroit Case ICC Rest Ch	Self-	80	Cers_ECC_Rest_CA	Cores_RCC_Root_CA
toweshilow. Indusc Academic and Research Institutions RootCA 2001	Self-	854	Indexiculations, and Jasen Multiples, Just 54, 201	1 Helesc, Andersc, and Desert Chattach
toward-byset CESTE VICENEY Shake Root SE CA	Self-	854	015TE_WCSeriex_Ghitei_Rook_GB_CA	01578_WESeries_Global_Root_08_CA
toreal-built Amazon Root Ck. 4	Sel-	ec.	Amazon_Root_CA_4	Amazon, Rost, CA, 4
Kompan Kruit <u>207 Rave CA X2</u>	Self-	854	007_Awt_C4_X3	DST_Root_CA_X3
Koncan Kruit Addituat External CA Root	Self-	854	AddTsat_Dremal_CA_Rott	AddTrust_External_CA_Root
toman trust <u>costors com</u>	Set-	83.4	op.ton.am	613-3678-00M
torcal trut Efficies Estation Can 3	ball-	124	P Tabilac_DobaRost_Class_3	Phradies_StokeRoot_Case_3
tonico trust <u>Distant distail toot da</u>	Sel-	63.0	DigiCert_Dobal_Root_S3	DigiCell_Stabel_Root_S2

(iii)选择证书,然后点击下载.PEM文件,将其保存在ADS服务器上的临时文件夹中。

## File Name ccp.bora.com.pem

	eeb.ee.ee.ee.ee.ee.
Certificate Purpose	tomcat-trust
Certificate Type	trust-certs
Certificate Group	product-cpi
Description(friendly name)	Trust Certificate

#### Certificate File Data



注意:对用户执行相同的步骤。

#### 步骤2.将VOS平台应用导入ADS服务器

运行密钥工具的路径:C:\Program文件(x86)\Java\jre1.8.0\_221\bin

### 导入自签名证书的命令:

keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0\_221\lib\security\cacerts" -import storepass changeit -alias {fqdn\_of\_vos} -file c:\temp\certs\vosapplicationX.cer

在ADS服务器上重新启动Apache Tomcat服务。

注意:在其他ADS服务器上执行相同任务

### 第3部分:Roggers、PG和ADS服务器之间的证书交换

成功完成此交换所需的步骤如下:

- 步骤 1:从Rogger和PG服务器导出IIS证书
- 步骤 2:从Rogger和PG服务器导出诊断框架门户(DFP)证书

步骤 3:将证书导入ADS服务器

#### 步骤1.从Rogger和PG服务器导出IIS证书

(i)在浏览器的ADS服务器上,导航至服务器(Roggers, PG)url:https://{servername}

(ii)将证书保存到临时文件夹,例如c:\temp\certs,并将证书命名为ICM{svr}[ab].cer

#### ← → C A Not secure aw125a.bora.com Certificate × General Details Certification Path 🖉 Certificate Export Waard he la serie de la 4-Sevi (Ab Export File Format Field Value Certificates can be exported in a variety of file formats Versor 12 Serial number 00 #9 #6 59 50; 75 46 75 85 Sgrature algorithm she256ASA Select the format you want to use: Sgrature hash algorithm \$4256 au 125a.bora.com O DER encoded binary X. 509 (LCER) Monday, September 30, 2019 vald from Base 64 encoded X.509 (CER) valid to Sunday, September 25, 2039 .... 125a hora ros Cryptographic Message Suntax Standard - PKCS #7 Certificates (JP78) S. Acars Include all certificates in the certification path if possible Personal Information Exchange - PRCS #12 (2PD) Include all certificates in the certification path if p Delete the private key if the export is successful Deport all extended properties Enable certificate privacy C Monasoft Serialized Centificate Store (1557) Copy to File

#### CCE via Chrome Browser

注意:选择选项Base-64 encoded X.509(.CER)。

#### 步骤2.从Rogger和PG服务器导出诊断框架门户(DFP)证书

(i)在浏览器的ADS服务器上,导航至服务器(Roggers, PGs)DFP URL:*https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion* 

#### (ii)将证书保存到文件夹示例c:\temp\certs,并将证书命名为dfp{svr}[ab].cer

Portico via Chrome Browser



注意:选择选项Base-64 encoded X.509(.CER)。

#### 步骤3.将证书导入ADS服务器

# 用于将IIS自签名证书导入ADS服务器的命令。运行Key工具的路径:C:\Program文件 (x86)\Java\jre1.8.0\_221\bin。

keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0\_221\lib\security\cacerts" -import storepass changeit -alias {fqdn\_of\_server}\_IIS -file c:\temp\certs\ ICM{svr}[ab].cer

Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0\_221\lib\security\cacerts" - import -storepass changeit -alias myrgra.domain.com\_IIS -file c:\temp\certs\ICMrgra.cer

#### 注意: 将导出的所有服务器证书导入所有ADS服务器。

#### 用于将诊断自签名证书导入ADS服务器的命令

keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0\_221\lib\security\cacerts" -import storepass changeit -alias {fqdn\_of\_server}\_DFP -file c:\temp\certs\ dfp{svr}[ab].cer

Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0\_221\lib\security\cacerts" - import -storepass changeit -alias myrgra.domain.com\_DFP -file c:\temp\certs\dfprgra.cer

#### 注意:将导出的所有服务器证书导入所有ADS服务器。

在ADS服务器上重新启动Apache Tomcat服务。

## 第4部分: CVP CallStudio WEBService集成

有关如何为Web服务元素和Rest\_Client元素建立安全通信的详细信息

请参阅《Cisco Unified CVP VXML服务器和Cisco Unified Call Studio版本12.5(1)- Web服务集成用 户指南》[Cisco Unified Customer Voice Portal] - Cisco

## 相关信息

- CVP配置指南:<u>CVP配置指南 安全</u>
- UCCE配置指南: <u>UCCE配置指南 安全</u>
- PCCE管理指南: PCE管理指南 安全
- UCCE自签名证书: <u>Exchange UCCE自签名证书</u>
- 在CCE 12.5(1)中安装并迁移到OpenJDK:CCE OpenJDK迁移
- 在CVP 12.5(1)中安装并迁移到OpenJDK:CVP OpenJDK迁移