Certificados com assinatura automática do Exchange em uma solução UCCE

Contents

Introdução Pré-requisitos Requisitos Componentes Utilizados Background Procedimento Servidores CCE AW e servidores de aplicativos principais CCE Seção 1: Troca de certificados entre roteador\logger, PG e servidor AW Seção 2: Intercâmbio de certificados entre aplicativos da plataforma VOS e o servidor AW Secvidor CVP OAMP e servidores de componentes CVP Seção 1: Troca de certificados entre o servidor CVP OAMP e o servidor CVP e os servidores de relatórios Seção 2: Troca de certificados entre o servidor CVP OAMP e os aplicativos da plataforma VOS Seção 3: Troca de certificados entre o servidores CVP e VVB Integração do serviço Web CallStudio do CVP Informações Relacionadas

Introdução

Este documento descreve como trocar certificados autoassinados na solução Unified Contact Center Enterprise (UCCE).

Contribuição de Anuj Bhatia, Robert Rogier e Ramiro Amaya, engenheiros do Cisco TAC

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- UCCE versão 12.5(1)
- Customer Voice Portal (CVP) versão 12.5 (1)
- Cisco Virtualized Voice Browser (VVB)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- UCCE 12.5(1)
- CVP 12.5(1)
- Cisco VB 12.5
- Console de operações do CVP (OAMP)
- CVP Novo OAMP (NOAMP)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório

específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Background

Em uma solução UCCE, a configuração de novos recursos que envolvem aplicativos centrais, como ROGGERs, Gateways Periféricos (PGs), Estações de Trabalho Administrativas (AW) / Servidores de Dados Administrativos (ADS), Finesse, Cisco Unified Intelligence Center (CUIC) e assim por diante, é feita através da página de Administração do Contact Center Enterprise (CCE). Para aplicativos de Resposta de Voz Interativa (IVR - Interative Voice Response) como CVP, Cisco VB e gateways, o NOAMP controla a configuração de novos recursos. A partir do CCE 12.5(1), devido à conformidade de gerenciamento de segurança (SRC), todas as comunicações para o CCE Admin e NOAMP são estritamente feitas através do protocolo HTTP seguro.

Para obter uma comunicação segura perfeita entre esses aplicativos em um ambiente de certificado autoassinado, a troca de certificados entre os servidores torna-se uma necessidade. A próxima seção explica em detalhes as etapas necessárias para trocar o certificado autoassinado entre:

- Servidores CCE AW e servidores de aplicativos principais CCE
- Servidor CVP OAMP e servidores de componentes CVP

Procedimento

Servidores CCE AW e servidores de aplicativos principais CCE

Estes são os componentes dos quais os certificados autoassinados são exportados e os componentes para os quais os certificados autoassinados precisam ser importados.

Servidores AW CCE: este servidor requer certificado de:

• Plataforma Windows: Roteador e Agente(Rogger){A/B}, Gateway Periférico (PG){A/B} e todos os AW/ADS.

Observação: o IIS e os certificados do Diagnostic Framework Portico (DFP) são necessários.

• Plataforma VOS: Finesse, CUIC, Live Data (LD), Identity Server (IDS), Cloud Connect e outros servidores aplicáveis que fazem parte do banco de dados de inventário.

O mesmo se aplica a outros servidores AW na solução.

Roteador \ Servidor de Log: Este servidor requer certificado de:

• Plataforma Windows: todos os certificados IIS do servidor AW.

As etapas necessárias para a troca eficaz de certificados autoassinados para o CCE estão divididas nestas seções:

Seção 1: Troca de certificados entre roteador\logger, PG e servidor AW Seção 2: Intercâmbio de certificados entre o aplicativo da plataforma VOS e o servidor AW

Seção 1: Troca de certificados entre roteador\logger, PG e servidor AW

As etapas necessárias para concluir essa troca com êxito são:

Etapa 1. Exporte certificados do IIS de Router\Logger, PG e todos os servidores AW.

- Etapa 2. Exporte certificados DFP de Router\Logger, PG e todos os servidores AW.
- Etapa 3. Importe certificados IIS e DFP de Router\Logger, PG e AW para servidores AW.

Etapa 4. Importe certificados do IIS para o Roteador\Agente de Log e PG dos servidores AW.

Cuidado: antes de começar, você deve fazer backup do armazenamento de chaves e abrir o prompt de comando como Administrador.

(i) Conheça o caminho do home do java para garantir onde o java keytool está hospedado. Há algumas maneiras de encontrar o caminho do início java.

Opção 1: Comando CLI: echo %JAVA_HOME%



Opção 2: manualmente, por meio da configuração Avançada do sistema, conforme mostrado na imagem.

🔶 🔶 👻 🛧 🔛 🤅 Control Par	nel > System and Security > System 🗸 💍 Sea	rch Co	ntrol Panel	
Control Panel Home	System Properties	×	e e e e e e e e e e e e e e e e e e e	`
 Device Manager Remote settings 	Computer Name Hardware Advanced Remote You must be logged on as an Administrator to make most of these changes.		Environment Variables	
Advanced system settings	Performance	S	User variables for Administrator	
	Visual ellects, processor scheduling, memory usage, and visual memory		Path	%USERPRO
	Liser Profiles	IG	TEMP	%USERPRO %USERPRO
	Desktop settings related to your sign-in	iso Dia		
	Startup and Recovery System startup, system failure, and debugging information			
	Settings		System variables	
	Environment Variables	1	Variable ComSpee	Value Ci\Window
		┛┠	JAVA_HOME JAVA_OPTS	C:\Program
See also	OK Cancel Apply		OS Activate Wind	6 Windows_N
Security and Maintenance			Path Go to Settings to	C:\icm\bin; .COM·.EXE:

Observação: no UCCE 12.5, o caminho padrão é C:\Program Files (x86)\Java\jre1.8.0_221\bin. No

entanto, se você tiver usado o instalador 12.5(1a) ou tiver o 12.5 ES55 instalado (OpenJDK ES obrigatório), use o %CCE_JAVA_HOME% em vez do %JAVA_HOME%, pois o caminho do armazenamento de dados foi alterado com o OpenJDK. Mais informações sobre a migração do OpenJDK no CCE e no CVP nestes documentos: Instalar e migrar para o OpenJDK no CCE 12.5(1) e Instalar e migrar para o OpenJDK no CVP 12.5(1).

(ii) Faça backup do arquivo **cacerts** da pasta **{JAVA_HOME}\lib\security.** Você pode copiá-lo para outro local.

Etapa 1. Exportar certificados do IIS de Router\Logger, PG e todos os servidores AW

(i) Em um servidor AW a partir de um navegador, navegue até os servidores (ROGGERs, PG, outros servidores AW) url: https://{servername}.

← → C A Not secure aw125a.bora.com			
Certificate X General Details Certification Path Show: All> Field Value Version V3 Serial number 00 a9 ab b9 bc 76 4b 76 8f Signature algorithm sha256RSA Signature hash algorithm sha256 Issuer aw 125a.bora.com Valid from Monday, September 30, 2019 Valid to Sunday, September 25, 2039 Subject aw 125a hora.com	d d def:	 Certificate Export Wizard Export File Format Certificates can be exported in a variety of file formats. Select the format you want to use: DER encoded binary X.509 (.CER) Base-64 encoded X.509 (.CER) Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P78) Indude all certificates in the certification path if possible Personal Information Exchange - PKCS #12 (.PFX) 	×
Edit Properties Copy to File		 Indude all certificates in the certification path if possible Delete the private key if the export is successful Export all extended properties Enable certificate privacy Microsoft Serialized Certificate Store (.SST) 	

CCE via Chrome Browser

(ii) Salve o certificado em uma pasta temporária, por exemplo c:\temp\certs e nomeie o certificado como ICM{svr}[ab].cer.

Nota:Selecione a opção X.509 (.CER) codificado na Base 64.

Etapa 2. Exportar certificados DFP de Router\Logger, PG e todos os servidores AW

(i) No servidor AW, abra um navegador e navegue até os servidores (Router, Logger ou ROGGERs, PGs, AWs) DFP url : https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion.

Portico via Chrome Browser

etfole ed DtMt Cethologie	-	XICFI	
ei olo	v	aifie *-	Er Conficate Export Ward
eld Version Seral number Signature algorithm	Value V3 37 ee 21 ell-63 25 fb ali-4a 71 sha25685A	n 194	Export File Named Certificates can be exported in a variety of file formats.
Sprature hash agorithin Issuer raild from raild to 5. Assert	sha256 an 125e bora.com Manday, September 30, 2019 Anday, September 30, 2029 1 au 125e bora.com		Select the forward you want to use:
			see of ended as and contract service or states and contract service or states and contracts and contracts and and - MCS #7 Certificates (#78) induce all certificates in the contracts path (#76)
			research internation buildings - MLS # (2 (PP)) Delets the private key if the export is successful
	Edit Properties Copy to Pile.		Disperit at entended properties Disple certificate privacy

(ii) Salve o certificado na pasta exemplo c:\temp\certs e nomeie o certificado como dfp{svr}[ab].cer

Observação: selecione a opção X.509 (.CER) codificado na Base 64.

Etapa 3. Importar certificados do IIS e DFP de Router\Logger, PG e AW para servidores AW

Observação: os comandos de exemplo usam a senha de keystore padrão de "changeit". Você deve alterar isso se tiver modificado a senha em seu sistema.

Comando para importar os certificados autoassinados do IIS para o servidor AW. O caminho para executar a Keytool: **%JAVA_HOME%\bin**:

```
keytool -keystore ...lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_IIS -file
Example: keytool -keystore ...lib\security\cacerts -import -storepass changeit -alias myrgra.domain.com_
```

Observação: importe todos os certificados de servidor exportados para todos os servidores AW.

Comando para importar os certificados autoassinados do DFP para servidores AW:

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_DFP -file
Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myrgra.domain.com_
```

Observação: importe todos os certificados de servidor exportados para todos os servidores AW.

Reinicie o serviço Apache Tomcat nos servidores AW.

Etapa 4. Importe certificados do IIS para o Roteador\Agente de Log e PG dos servidores AW.

Comando para importar os certificados autoassinados do AW IIS para os servidores Router\Logger e PG:

```
keytool -keystore ...lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_IIS -file
Example: keytool -keystore ...lib\security\cacerts -import -storepass changeit -alias myawa.domain.com_I
```

Observação: importe todos os certificados do servidor AW IIS exportados para os servidores Router\Logger e PG nos lados A e B.

Reinicie o serviço Apache Tomcat nos servidores Router\Logger e PG.

Seção 2: Intercâmbio de certificados entre aplicativos da plataforma VOS e o servidor AW

As etapas necessárias para concluir essa troca com êxito são:

Etapa 1. Exportar certificados do servidor de aplicativos da plataforma VOS. Etapa 2. Importar certificados de aplicativos da plataforma VOS para o AW Server.

Esse processo se aplica a todos os aplicativos de VOS, como:

- Finesse
- CUIC \setminus LD \setminus IDS
- Conexão em nuvem

Etapa 1. Exportar certificados do servidor de aplicativos da plataforma VOS.

(i) Navegue até a página Cisco Unified Communications Operating System Administration: https://{FQDN}:8443/cmplatform.

(ii) Navegue para **Segurança** > **Gerenciamento de Certificados** e localize os certificados do servidor primário de aplicativos na pasta tomcat-trust.

dudy. Cisco Unified Operating System Admin For Case Unified Communications Solutions	nistrati	on		Anterior Cours Under OS Adversariation •
Cartificate List				
🖳 Generale Self-agenti 🎧 lipical Cathode Cathode dan 🔠 Generale	CSR			
toreal-trust Case ECC Rest, CA	Sal-	ec.	Com, #CC, Aust, CA	Coox_ECC_Avet_CA
towest-bust palanic Academic and Research Institutions RootlA 2011	Sall-	854	Nelevic,Academic,and,Research,Institutions,RootCA,201	Mellenic, Academic, and , Research, Smithub
toward-trust costs utiliaries, Stated Aust, SB, CA	Sal-	RSA	01578_W15eKey_Globel_Rook_GB_CA	00578_WDerkey_Global_Root_GB_CA
tomost-trust Amazon Root CA.4	Saf-	ec.	Amazon_Root_CA_4	Amazon, Root, CA, 4
tomat-trust 017 Revt CA 32	Self-	854	DST_RevE_CA_X3	DST_Reet_CA_X3
toreal-tout <u>Additud External CA Red</u>	Self-	RSA	AddTrust_External_CA_Root	AddTrust_External_CA_Root
tampat-trust couloca.com	Daff-	854	op-box.com	capitors.com
toreat-tool <u>Efficient Colaitant Case 3</u>	Sail-	83A	* Telefac_GrobalHoot_Class_3	T-felelet_Gobalkoot_Cass_3
turnat-trust DisiCart Clobal Root G2	Self	124	DigiCert_Global_Root_G3	DipiCert_Global_Root_G2

(iii) Selecione o certificado e clique em baixar arquivo .PEM para salvá-lo em uma pasta temporária no servidor AW.

Certificat	e Settings		_
File Name		ccp.bora.com.pem	
Certificate	Purpose	tomcat-trust	
Certificate	Type	trust-certs	
Certificate	Group	product-cpi	
Descriptio	n(friendly name)	Trust Certificate	
- Certifical	e File Data		_
[Version Serial N Signatu Issuer N Validity T Subject Key va 3082010 69f9980a 88e0e81 f140216a 520da30	V3 umber: SC35B3A reAlgorithm: SHA lame: L=BXB, ST From: Non Dec: Do: Sat Dec 14 1 Name: L=BXB, S 4 (1.2.840.1135 lue: s0282010100c14 1246814be9a3c1 be64ad44c39f00 Se5aca1787b14 s39b206d213b32 Download .PEM	189A8974719B885B6A92CF710D 1256withRSA (1.2.840.113549.1.11) =ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 16 10:55:22 EST 2019 0:55:21 EST 2024 17=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US 49.1.1.1) 20ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199 556a8401237c1d980b09a05903520b0013b30f54fbfdda3e71f27900d992 2162aadcbc08f591a960cef95eda7b86b3e6e183a2fe8732352aee5abcfb722 2162aadcbc08f591a960cef95eda7b86b3e6e183a2fe8732352aee5abcfb72 2162aadcbc08f591a960cef95eda7b86b3e6e183a2fe8732352aee5abcfb722 2162aadcbc08f591a960cef95eda7b86b3e6e183a2fe8732352aee5abcfb722 2162aadcbc08f591a960cef95eda7b86b3e6e183a2fe8732352aee5abcfb722 2162aadcbc08f591a960cef95eda7b86b3e6e183a2fe8732352aee5abcfb722 2162aadcbc08f591a960cef95eda7b86b3e6e183a2fe8732352aee5abcfb722 2162aadcbc08f591a960cef95eda7b86b3e6e183a2fe8732352aee5abcfb722 2162aadcbc08f591a960cef95e61b6d6dcf4291668a2ee660d72ba0c3ccf85444f7a 1File Download .DER File	•

Observação: Execute as mesmas etapas para o assinante.

Etapa 2. Importe o aplicativo da plataforma VOS para o AW Server.

Caminho para executar a ferramenta de Chave: {JAVA_HOME}\bin

Comando para importar os certificados autoassinados:

keytool -keystore ...lib\security\cacerts -import -storepass changeit -alias {fqdn_of_vos} -file c:\temp

Reinicie o serviço Apache Tomcat nos servidores AW.

Observação: execute a mesma tarefa em outros servidores AW.

Servidor CVP OAMP e servidores de componentes CVP

Estes são os componentes dos quais os certificados autoassinados são exportados e os componentes para os quais os certificados autoassinados precisam ser importados.

(i) Servidor CVP OAMP: este servidor exige certificado de:

- Plataforma Windows: certificado do Gerenciador de Serviços Web (WSM) do servidor CVP e dos servidores de Relatórios.
- Plataforma VOS: Cisco VB para integração com o Customer Virtual Agent (CVA), servidor Cloud Connect para integração com o Webex Experience Management (WXM).

(ii) Servidores CVP: Este servidor requer certificado de:

- Plataforma Windows: certificado WSM do servidor OAMP.
- Plataforma VOS: servidor Cloud Connect para integração WXM e servidor Cisco VVB.

(iii) Servidores de relatórios do CVP: este servidor exige certificado do

• Plataforma Windows: certificado WSM do servidor OAMP.

(iv) servidores Cisco VB:este servidor requer certificado de:

• Plataforma Windows: certificado VXML do servidor CVP e certificado Callserver do servidor CVP.

As etapas necessárias para a troca eficaz de certificados autoassinados no ambiente do CVP são explicadas nessas três seções.

Seção 1: Troca de certificados entre o servidor CVP OAMP e o servidor CVP e os servidores de relatórios. Seção 2: Intercâmbio de certificados entre o servidor CVP OAMP e os aplicativos da plataforma VOS. Seção 3: Troca de certificados entre o servidor CVP e os servidores VVB.

Seção 1: Troca de certificados entre o servidor CVP OAMP e o servidor CVP e os servidores de relatórios

As etapas necessárias para concluir essa troca com êxito são:

Etapa 1. Exporte o certificado WSM do servidor CVP, do servidor de relatórios e do servidor OAMP. Etapa 2. Importe certificados WSM do servidor CVP e do servidor de Relatórios para o servidor OAMP. Etapa 3. Importe o certificado WSM do servidor CVP OAMP para o servidor CVP e o servidor de relatórios.

Cuidado: antes de começar, você deve fazer o seguinte:

1. Abra uma janela de comando como administrador.

2. Para identificar a senha do armazenamento de chaves, execute o comando, more

%CVP_HOME%\conf\security.properties.

3. Você precisa dessa senha ao executar os comandos keytool.

4. No diretório %CVP_HOME%\conf\security\, execute o comando copy .keystore

backup.keystore.

Etapa 1. Exporte o certificado WSM do servidor CVP, do servidor de relatórios e do servidor OAMP.

(i) Exporte o certificado WSM de cada servidor para um local temporário e renomeie o certificado com um nome desejado. Você pode renomeá-lo como wsmX.crt. Substitua X pelo nome de host do servidor. Por exemplo, wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt, wsmoamp.crt.

Comando para exportar os certificados autoassinados:

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

(ii) Copie o certificado do caminho C:\Cisco\CVP\conf\security\wsm.crt de cada servidor e renomeie-o como wsmX.crt com base no tipo de servidor.

Etapa 2. Importe os certificados WSM dos servidores CVP e dos servidores de relatórios para o servidor OAMP.

(i) Copie o certificado WSM de cada servidor CVP e servidor de Relatórios (wsmX.crt) para o diretório %CVP_HOME%\conf\security no servidor OAMP.

(ii) Importe esses certificados com o comando:

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

(iii) Reinicialize o servidor.

Etapa 3. Importe o certificado WSM do servidor CVP OAMP para os servidores CVP e servidores de relatórios.

(i) Copie o certificado WSM do servidor OAMP (wsmoampX.crt) para o diretório %CVP_HOME%\conf\security em todos os servidores CVP e servidores de Relatórios.

(ii) Importar os certificados com o comando:

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

(iii) Reinicialize os servidores.

Seção 2: Troca de certificados entre o servidor CVP OAMP e os aplicativos da plataforma VOS

As etapas necessárias para concluir essa troca com êxito são:

Etapa 1. Exporte o certificado do aplicativo da plataforma VOS.

Etapa 2. Importe o certificado do aplicativo VOS para o servidor OAMP.

Esse processo é aplicável a aplicativos VOS, como:

- CUCM
- VVB
- Conexão em nuvem

Etapa 1. Exporte o certificado do aplicativo da plataforma VOS.

(i) Navegue até a página Cisco Unified Communications Operating System Administration: <u>https://{FQDN}:8443/cmplatform</u>.

(ii) Navegue para **Segurança** > **Gerenciamento de Certificados** e localize os certificados do servidor primário de aplicativos na pasta tomcat-trust.

Certificate Li	M				
🖳 Cerente	Set ayout 🖓 Uptac Catholic Catholic Asia 限 Catalo	COR			
		signed			
tomost-trust	theste, Rimery, Root, CA, 62	Saf-	RSA	theads_himary_Rod_GA63	thanks_himary_Root_CAG0
tomost-trust	Subalive	Safe signed	90	Clubal Sign	GabelSign
tomost-trust	EE Certification Centre Root, CA	Sall-	RSA	EE_Certification_Certine_Root_CA	BE_Certification_Centre_Root_CA
tomost-trust	SinkerSter, Aust. CA	Sall-	R5A	GlobalSign_Root_CA	Gobe/Sign_Root_CA
formal trust	TRCA Rest Certification Authority	Saf-	RSA	TeCA_Root_Certification_Authority	TeCs_Root_Certification_Authority
tomost-trust	Bavenue Case 3 Root CA	Sall- signed	854	Buypens_Cees_3_Root_CA	Bogen, Cen, J. Art, CA
tomost-trust	Staffeld Services Root Catificate Authority - 62	Saf-	R.SA	Darfeld_Bervices_Root_Certificate_AuthorityG2	Starfield_Bervices_Root_Certificate_Authority62
tempet-trust	Verbier, Dass 3. Addic Arimary, Cathletion, Authority, 1	545	854	terdion_Case_3_hblic_himary_Cartification_Authority	VeriSign_Class_3_Public_Primary_Certification_Authority
tomost-trust	whill ben com	Salt- signed	854	Indiana Jan	while how com
tomost-trust	Stars, Cuba, Celtifiator, Aultority	Saf-	854	Mang_Oldar_Cellfrator_Autority	Xtany_Dida(_Cellification_Authority

(iii) Selecione o certificado e clique em fazer download do arquivo .PEM para salvá-lo em uma pasta temporária no servidor OAMP.

Status	
i Status: Ready	
Certificate Settings –	
File Name	vvb125.bora.com.pem
Certificate Purpose	tomcat-trust
Certificate Type	trust-certs
Certificate Group	product-cpi
Description(friendly na	me) Trust Certificate
Version: V3 Serial Number: 68FE SignatureAlgorithm: Issuer Name: L=rtp, Validity From: Thu D To: Tue Dec O Subject Name: L=rtp	S5F56F8631108440835882508403 SHA256withRSA (1.2.840.113549.1.1.11) ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US ec 05 06:51:10 PST 2024 03 06:51:10 PST 2024 . ST=nc. CN=vvb125.bora.com, OU=lab, O=bora, C=US
Key: RSA (1.2.840.1 Key value: 3082010a0282010100 9fe42726c826e36113 7096e81d65bdcd0cad a911b95cf7dbc9c9e27 c77de1da40e15f1c0ae	13549.1.1.1) f16d44864befb1687cc517f06c3af77d9d66db719f9dbee922051be3bc7578bb 207d187db01780d0d7b1b38462c7df77fa97f17e87e0408077b556ffc2c00065 bcbdddf1df1d9ad0975a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c 09d1d761b52fdb2aa7df0b2db7f8d2449ef252fefc7561f1b042345358f25009e 40bc03dd815ceab5fc46a00daccd81013bd693614684c27e05de2004553004
Delete Download .	PEM File Download .DER File

Etapa 2. Importe o certificado do aplicativo VOS para o servidor OAMP.

(i) Copie o certificado VOS para o diretório %CVP_HOME%\conf\security no servidor OAMP.

(ii) Importar os certificados com o comando:

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

(ii) Reinicialize o servidor.

Seção 3: Troca de certificados entre servidores CVP e VVB

Esta é uma etapa opcional para proteger a comunicação SIP entre o CVP e outros componentes do Contact Center. Para obter mais informações consulte a seção Guia de configuração do CVP: <u>Guia de configuração do CVP - Segurança</u>.

Integração do serviço Web CallStudio do CVP

Para obter informações detalhadas sobre como estabelecer uma comunicação segura para o elemento de serviços da Web e o elemento Rest_Client

Consulte o <u>Guia do usuário do Cisco Unified CVP VXML Server e do Cisco Unified Call Studio Release</u> 12.5(1) - Integração de serviços da Web [Cisco Unified Customer Voice Portal] - Cisco

Informações Relacionadas

- Guia de configuração do CVP Segurança
- Guia de segurança do UCCE
- Guia do administrador do PCCE Segurança
- <u>Certificados com assinatura automática do Exchange PCCE PCCE 12.5</u>
- <u>Certificados com assinatura automática do Exchange UCCE UCCE 12.5</u>
- Certificados com assinatura automática do Exchange PCCE PCCE 12.6

- Implementar certificados assinados por CA CCE 12.6
 Migração OpenJDK do CCE

- <u>Migração OpenJDK do CVP</u>
 <u>Suporte Técnico e Documentação Cisco Systems</u>

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.