Implementar certificados CA assinados em uma solução CCE

Contents

Introdução Pré-requisitos **Requisitos** Componentes Utilizados Background Procedimento Servidores baseados em Windows CCE 1. Gerar CSR 2. Obter os Certificados Assinados pela CA 3. Carregar os Certificados Assinados pela CA 4. Associar o Certificado Assinado pela CA ao IIS 5. Vincular o Certificado Assinado pela CA ao Pórtico de Diagnóstico 6. Importe o Certificado Raiz e Intermediário para o Armazenamento de Chaves Java Solução CVP 1. Gerar Certificados com FQDN 2. Gerar o CSR 3. Obter os Certificados Assinados pela CA 4. Importar os Certificados Assinados pela CA Servidores VOS 1. Gerar Certificado CSR 2. Obter os Certificados Assinados pela CA 3. Carregar o Aplicativo e Certificados Raiz Verificar Troubleshooting Informaçõesrelacionadas

Introdução

Este documento descreve como implementar certificados assinados de Autoridade de certificação (CA) na solução Cisco Contact Center Enterprise (CCE).

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:

- Unified Contact Center Enterprise (UCCE) versão 12.5(1)
- Package Contact Center Enterprise Versão 12.5(1)
- Customer Voice Portal (CVP) versão 12.5 (1)
- Cisco Virtualized Voice Browser (VVB)
- · Console de operações e administração (OAMP) do Cisco CVP
- Cisco Unified Intelligence Center (CUIC)
- Cisco Unified Communication Manager (CUCM)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- PCCE 12.5(1)
- CVP 12.5(1)
- Cisco VB 12.5
- Finesss 12,5
- CUIC 12.5
- Windows 2016

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

Os certificados são usados para garantir que a comunicação seja segura com a autenticação entre clientes e servidores.

Os usuários podem comprar certificados de uma CA ou usar certificados autoassinados.

Os certificados autoassinados (como o nome indica) são assinados pela mesma entidade cuja identidade eles certificam, ao contrário de serem assinados por uma autoridade de certificação. Os certificados autoassinados não são considerados tão seguros quanto os certificados de CA, mas são usados por padrão em muitos aplicativos.

Na versão 12.x da solução Package Contact Center Enterprise (PCCE), todos os componentes da solução são controlados pelo Single Pane of Glass (SPOG), que está hospedado no servidor principal da Admin Workstation (AW).

Devido à Conformidade de Gerenciamento de Segurança (SRC - Security Management Compliance) na versão PCCE 12.5(1), toda a comunicação entre o SPOG e outros componentes na solução é feita através do protocolo HTTP seguro. Na UCCE 12.5, a comunicação entre componentes também é feita através do protocolo HTTP seguro.

Este documento explica em detalhes as etapas necessárias para implementar certificados

assinados CA em uma solução CCE para comunicação HTTP segura. Para quaisquer outras considerações de segurança do UCCE, consulte <u>Diretrizes de segurança do UCCE</u>. Para qualquer comunicação segura CVP adicional diferente do HTTP seguro, consulte as diretrizes de segurança no guia de configuração do CVP: <u>Diretrizes de segurança do CVP</u>.

Procedimento

Servidores baseados em Windows CCE

1. Gerar CSR

Este procedimento explica como gerar uma CSR (Certificate Signing Request, Solicitação de Assinatura de Certificado) a partir do Gerenciador dos Serviços de Informações da Internet (IIS).

Etapa 1. Faça logon no Windows e escolha Painel de Controle > Ferramentas Administrativas > Gerenciador dos Serviços de Informações da Internet (IIS).

Etapa 2. No painel Conexões, clique no nome do servidor. O painel Início do servidor é exibido.



Etapa 3. Na área do IIS, clique duas vezes em Certificados do Servidor.



Etapa 4. No painel Ações, clique em Criar solicitação de certificado.

Connections Actions Q - Q - Q - Q - Q - Q - Q - Q - Q - Q -	icent

Etapa 5. Na caixa de diálogo Solicitar Certificado, faça o seguinte:

Especifique as informações necessárias nos campos exibidos e clique em Avançar.

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	

Na lista suspensa Provedor de serviços de criptografia, deixe a configuração padrão.

Na lista suspensa Tamanho do bit, selecione 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 the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance. Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider v Bit length: 2048	et	
		_
Previous Next Finish	Cancel	

Etapa 6. Especifique um nome de arquivo para a solicitação de certificado e clique em Concluir.

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

2. Obter os Certificados Assinados pela CA

Etapa 1. Assinar o certificado em uma CA.

Solution Construcção: certifique-se de que o modelo de certificado usado pela autoridade de certificação inclua autenticação de cliente e servidor.

Etapa 2. Obtenha os certificados CA assinados de sua autoridade de certificação (raiz, aplicativo e intermediário, se houver).

3. Carregar os Certificados Assinados pela CA

Etapa 1. Faça logon no Windows e escolha Painel de Controle > Ferramentas Administrativas > Gerenciador dos Serviços de Informações da Internet (IIS).



Etapa 2. No painel Conexões, clique no nome do servidor.

Connections Q,- 🔜 (名) (Q,	🖣 PC	CEAWA H	ome				
Start Page PCCEAWA (PCCERCON/pcceadmin)	Filter		• \$ 60 -	Show All	Group by:		
	Connection Strings	SMTP E-mail					•
	Authentic	Compression	Default	Directory Browsing	Error Pages	Handler Mappings	
	HTTP Redirect	HTTP Respon	ISAPI and CGI Restri	SAPI Filters	Logging	MML Types	
	And when the second sec	Cutput Caching	Request Filtering	Server Certificates	Worker Processes		
	Manageme	1	E			A	

Etapa 3. Na área do IIS, clique duas vezes em Certificados do Servidor.



Etapa 4. No painel Ações, clique em Concluir solicitação de certificado.

File View Help				
Connex/Sons	Games Castillan	ter.		Actions
Q. · 🖾 (🖄 (🖗 .	- server cerunca	0.05		import
Sant Page PCCEAREA (PCCERCDN/pcceadmin)	Use this feature to request and mo websites configured for SSL	anage certificates that the lifeb ser	ver can use with	Create Cetificate Request Complete Cetificate Request
	Filter + 17	Go - 😨 Show All Group by:		Create Domain Certificate
	Name *	Issued To	Issued By	Create Self-Signed Certificate
	Cisca ICM Diagnostic Framew	PCCEANA.PCCERCDN.cisco.c	PCCEANA/PCCERCE	Enable Automatic Rebind of
	Cisca ICM SSL Certificate	PCCLARA.PCCDRCDN.cscot	PCCEANA.PCCERCI	Renewed Certificate

Etapa 5. Na caixa de diálogo Concluir Solicitação de Certificado, preencha estes campos:

No campo Nome do arquivo que contém a resposta da autoridade de certificação, clique no botão

Navegue até o local onde o certificado de aplicativo assinado está armazenado e clique em Abrir.

Observação: se esta for uma implementação de CA de 2 camadas e o certificado raiz ainda não estiver no repositório de certificados do servidor, a raiz precisará ser carregada no Windows Store antes de você importar o certificado assinado. Consulte este documento se precisar carregar a CA raiz na Windows Store <u>https://docs.microsoft.com/en-us/skypesdk/sdn/articles/installing-the-trusted-root-certificate</u>. No campo Nome amigável, insira o FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado) do servidor ou qualquer nome significativo para você. Certifique-se de que a lista suspensa Selecionar um repositório de certificados para o novo certificado permaneça como Pessoal.

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

Etapa 6. Clique em OK para carregar o certificado.

Se o carregamento do certificado for bem-sucedido, o certificado será exibido no painel Certificados do Servidor.



4. Associar o Certificado Assinado pela CA ao IIS

Este procedimento explica como vincular um certificado assinado pela CA no Gerenciador do IIS.

Etapa 1. Faça logon no Windows e escolha Painel de Controle > Ferramentas Administrativas > Gerenciador dos Serviços de Informações da Internet (IIS).



Etapa 2. No painel Conexões, escolha <server_name> > Sites > Site padrão da Web.



Etapa 3. No painel Ações, clique em Vinculações....

internet information Services (IS) Manager								-	0	ж
😥 🛊 FCCEAWA + Sites + Default Web Site +									89	
File View Help										
Connections	Del Filter ASP.NET	fault Web	Site Hor	me 2 Show All Q	Group by:	Ē	Liptor Edit Pr Edit S Edit S Edit S Edit S	t erreissier Ne Sectionge	•	
	AET huthorizet Connection Strings	All Compilation	MET Error Pages	NET Outplanion	MET Inut Levels	Application Settings	View J View V Antope W S Restart Stop	legilicatio Artual De Rebuite	edories	
	Authentic HTTP Redirect Gulput	Compension HTTP Respon Respon	Default Decument SAAN Filters	Cirectory Breasing Logging	Error Pages Jime MMAC Types	Hander Magings Angelings Modules	Brown E Brown Advan Config Limbs Help	e Websi e 1980 (he e 1948) (he cost Setti pare m	ke tel rijel rijel	

Etapa 4. Clique no tipo https com a porta 443 e clique em Editar....

File View Help					
Connections		On Contrast Mich	Citationa		Actions
Q, - 🔄 🙇 😡. Ng Start Page	Ste Bindings	Co Default Web	site Home	7 X	Deptore Edit Permissions
Application Pools State State	Type Host Name http: Migs	Port IP Address 80 443	Binding Informa	Add	Bedrop: Best Settings.
				Remove	View Applications View Virtual Directories
				Browse	Manage Website
L L		0	0	Core	e Help
		Cutput Request	SSL Settings	×	
A					en .

Etapa 5. Na lista suspensa Certificado SSL, selecione o certificado com o mesmo nome amigável fornecido na etapa anterior.

Ng Internet Information Services (IS) Manager	- 0 X
(+	🖬 🖂 🔒 🔒 •
File View Help	
Connections Default Main City Harman	Actions
Q. Li 🖄 😥	🔁 Deploye
Stat Page	Lét Permissions
Application Peols Type Host Name Port IP Address Binding Informa. Add.	1.61 514
V 2 Stel http 80 *	Tesc Settings.
	Yes Applications
- Amore	Vew Virtual Directories
Car see Ending	Manage Website 🛞
Type IP address Part	2 Resart
https://www.international.com	9 See
Hod name	Browse Website
	🕱 Browse 100 (Http)
Require Server Name Indication	Erowse (40 (https)
	Advanced Settings
33L certificate	Configure
CCLARA.pccercds.cico.com v Select View	0.000
OK Cancel	
DC Testures View Content New	-
Fasty	

Etapa 6. Click OK.

Passo 7. Navegue até Start > Run > services.msc e reinicie o IIS Admin Service.

Q, Sevices					- 0	x
File Action View	Help					
🕈 🌩 🚾 🖬 🖄	🔒 🖬 🕾 🖛 💷 📄					
Q, Senices (Local)	 Services (Local) 					
	Agache Tomost 9	Name	Description	Status	Statup Type	Log of
		Control of the American Service	Provides a mechanism to exchange data betwee		Manual (Trip	1.04
	Sog the service	C. Hyper-V Guest Service Interface	Provides an interface for the Hyper-Wheat to int		Manual (Trip	Los
	Restart the service	C. Hyper-Y Guest Shutdown Service	Provides a mechanism to shut down the operation		Manual (Trip	Los
		C. Hyper-Y Heartbeat Service	Monitors the state of this virtual machine by rep		Manual (Trip.,	Los
	Description	Appenty PowerShell Direct Service	Provides a mechanism to manage virtual machi		Manual (Trip	1.04
	Apache Tomost \$0 Server -	Q Hyper-Y Remote Desistop Virtualizatio	Provides a platform for communication betwee		Manual (Trig.,	Los_
	http://tomcat.apache.org/tomcat/	Q Hyper-V Time Synchronization Service	Synchronizes the system time of this virtual mac		Manual (Trig.,	Les n.
		C. Hyper V Volume Shadow Copy Reput	Coordinates the communications that are requir		Manual (Trip.,	Los -
		15 Admin Senice	Enables this server to administer the IS metabas	Renning	Automatic	Los
		12 KE and Authill Part Laying Modules	The REECT service heats the Internet Key Excha-	Renning	Automatic (T.,	Les
		Childrenotive Services Detection	Enables user notification of user input for intera		Pisabled	Los
		Chinternet Connection Sharing (CS)	Provides network address translation, addressin		Disabled	Los
		Q.P Helper	Provides turnel connectivity using Pv6 transitio-	Renting	Automatic	Los
		C. Post Policy Agent	Internet Protocol security (Poec) supports netw	Running	Manual (Trip.,	No
		ADC Provy Server service (KPS)	KDC Proxy Server service runs on edge servers to		Manual	No
		Chamber for Distributed Instruction C	Coordinates transactions between the Distribute		Manual (Trigge	Ne

Se o IIS for reiniciado com êxito, os avisos de erro de certificado não serão exibidos quando o aplicativo for iniciado.

5. Vincular o Certificado Assinado pela CA ao Pórtico de Diagnóstico

Este procedimento explica como vincular um CA Signed Certificate ao Diagnostic Portico.

Etapa 1. Abra o prompt de comando (Executar como administrador).

Etapa 2. Navegue até a pasta inicial do Diagnostic Portico. Execute este comando:

cd c:\icm\serviceability\diagnostics\bin

Etapa 3. Remova a associação de certificado atual ao Pórtico de Diagnóstico. Execute este comando:

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>_

Etapa 4. Abra o certificado assinado e copie o conteúdo de hash (sem espaços) do campo Impressão digital.

Certificate	×
General Details Certification Path	
Show: <all></all>	
FieldValueAuthority Key IdentifierKeyID = 03 2f 51 0CRL Distribution Points[1]CRL DistributionAuthority Information Access[1]Authority InfoCertificate Template InformTemplate = CC WebApplication Policies[1]Application Certification CertificateKey UsageDigital Signature, IThumbprint algorithmsha1Thumbprint97 93 74 00 99 19	Access: Acc b Server(1.3 tificate Polic Key Encipher 53 d6 4e 0b
97 93 74 00 99 19 53 d6 4e 0b c5 96 36 dc 4b cb Edit Properties	6e c4 4c bd
	OK

Etapa 5. Execute este comando e cole o conteúdo de hash.



Se a associação de certificado for bem-sucedida, será exibida a mensagem A associação de certificado é VÁLIDA.

Etapa 6. Valide se a associação de certificado foi bem-sucedida. Execute este comando:

DiagFwCertMgr /task:ValidateCertBinding



Observação: DiagFwCertMgr usa a porta 7890 por padrão.

Se a associação de certificado for bem-sucedida, será exibida a mensagem A associação de

certificado é VÁLIDA.

Passo 7. Reinicie o serviço Estrutura de Diagnóstico. Execute estes comandos:

net stop DiagFwSvc net start DiagFwSvc

Se o Diagnostic Framework for reiniciado com êxito, os avisos de erro de certificado não serão exibidos quando o aplicativo for iniciado.

6. Importe o Certificado Raiz e Intermediário para o Armazenamento de Chaves Java

Cuidado: antes de começar, você deve fazer backup do armazenamento de chaves e executar os comandos a partir do java home como um Administrador.

Etapa 1. Conheça o caminho do home do java para garantir onde o keytool do java está hospedado. Há algumas maneiras de encontrar o caminho do início java.

Opção 1: Comando CLI: echo %JAVA_HOME%



Opção 2: manualmente via configuração de sistema avançada, como mostrado na imagem

🔶 🔶 👻 🛧 🔛 🤉 Control Par	nel > System and Security > System v Ö Sea	arch Co	ontrol Panel	٩	×
Control Panel Home	System Properties	×		•	^
Device Manager	Computer Name Hardware Advanced Remote	_	Environment	Variables	
Advanced system settings	You must be logged on as an Administrator to make most of these changes. Performance	s	User variat	bles for Administra	tor
	Visual effects, processor scheduling, memory usage, and virtual memory		Variable		Value
			Path		%USERPROFILE%\AppData\Lc
	Settings	IG	TEMP		%USERPROFILE%\AppData\Lo
	Llear Profilae		TMP		%USERPROFILE%\AppData\Lc
	Desktop settings related to your sign-in				
	Desired astringenoided to your agrini	iso	0		
	Settings	Di	i:		
	Startup and Recovery System startup, system failure, and debugging information				Net
	Settings		System var	riables	
		411	Variable		Value
	Environment Variables		ComSpe		Ci\Windows\system32\emde
	L	<u>ا ا</u> د	JAVA_HO	OME	C:\Program Files (x86)\Java\j
		-	JAVA_OF	PTS	-Dbundle.provider.className
	OK Cancel Apply		NUMBER	R_OF_PROCESSOR	S 6
See also	FT0000010-00370-30063-00431-44503		OS	Activate W	ind Windows_NT
Security and Maintenance			Path	Go to Settings	C:\icm\bin:%JAVA_HOME%\b
			PATHEX	T	.COM:.EXE:.BAT:.CMD:.VBS:.VE

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 (obrigatório OpenJDK ES), use CCE_JAVA_HOME em vez de JAVA_HOME, pois o caminho do armazenamento de dados foi alterado com OpenJDK. Mais informações sobre a migração do OpenJDK no CCE e no CVP nestes documentos: Instalar e migrar para o OpenJDK no CCE 2.5(1) e Instalar e migrar para o OpenJDK no CVP 12.5(1).

Etapa 2. Faça backup do arquivo cacerts da pasta C:\Program Files (x86)\Java\jre1.8.0_221\lib\security. Você pode copiá-lo para outro local.

Etapa 3. Abra uma janela de comando como Administrador para executar o comando:

keytool.exe -keystore ./cacerts -import -file <path where the Root, or Intermediate certificate are sto

Observação: os certificados específicos necessários dependem da autoridade de certificação que você usa para assinar seus certificados. Em uma autoridade de certificação de dois níveis, que é típica de autoridades de certificação públicas e mais segura do que as internas, você precisa importar os certificados raiz e intermediários. Em uma CA autônoma sem intermediários, que geralmente é vista em um laboratório ou em uma CA interna mais simples, você só precisa importar o certificado raiz.

Solução CVP

1. Gerar Certificados com FQDN

Este procedimento explica como gerar certificados com o FQDN para os serviços Web Service Manager (WSM), Voice XML (VXML), Call Server e Operations Management (OAMP).

Observação: quando você instala o CVP, o nome do certificado inclui apenas o nome do servidor e não o FQDN, portanto, você precisa gerar novamente os certificados.

 Cuidado: antes de começar, você deve fazer o seguinte:
 1. Obtenha a senha do armazenamento de chaves. Execute o comando: more %CVP_HOME%\conf\security.properties. Essa senha é necessária ao executar os comandos keytool.

2. Copie a pasta %CVP_HOME%\conf\security para outra pasta.

3. Abra uma janela de comando como Administrador para executar os comandos.

Servidores CVP

Etapa 1. Para excluir os servidores CVP, os certificados executam estes comandos:

```
%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
```

Digite a senha do armazenamento de chaves quando solicitado.

Etapa 2. Para gerar o certificado WSM, execute este comando:

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

Digite a senha do armazenamento de chaves quando solicitado.

Observação: por padrão, os certificados são gerados por dois anos. Use -valid XXXX para definir a data de expiração quando os certificados forem gerados novamente; caso contrário, os certificados serão válidos por 90 dias e precisarão ser assinados por uma CA antes dessa data. Para a maioria desses certificados, 3 a 5 anos devem ser um tempo de validação razoável. Aqui estão algumas entradas de validade padrão:

Um ano	365
Dois anos	730
Três anos	1095
Quatro anos	1460
Cinco anos	1895
Dez anos	3650

Cuidado: em 12.5, os certificados devem ser SHA 256, Key Size 2048 e encryption Algorithm RSA, use estes parâmetros para definir estes valores: -keyalg RSA e -keysize 2048. É importante que os comandos keystore do CVP incluam o parâmetro -storetype JCEKS. Se isso não for feito, o certificado, a chave, ou pior, o armazenamento de chaves pode se tornar corrompido.

Especifique o FQDN do servidor na pergunta qual é seu nome e sobrenome?



Responda a estas outras perguntas:

Qual é o nome da sua unidade organizacional?

[Desconhecido]: <especificar UO>

Qual é o nome da sua empresa?

[Desconhecido]: <especifique o nome da organização>

Qual é o nome da sua cidade ou localidade?

[Desconhecido]: <especifique o nome da cidade/localidade>

Qual é o nome do seu estado ou província?

[Desconhecido]: <especifique o nome do estado/província> Qual é o código de duas letras do país para essa unidade? [Desconhecido]: <especifique o código de país com duas letras> Especifique yes para as duas próximas entradas.

Etapa 3. Execute as mesmas etapas para vxml_certificate e callserver_certificate:

%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

servidor de relatórios CVP

Etapa 1. Para excluir o WSM e os certificados do servidor de relatórios, execute estes comandos:

%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

Digite a senha do armazenamento de chaves quando solicitado.

Etapa 2. Para gerar o certificado WSM, execute este comando:

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

Digite a senha do armazenamento de chaves quando solicitado.

Especifique o FQDN do servidor para a consulta qual é seu nome e sobrenome? e continue com as mesmas etapas como feito com os servidores CVP.

Etapa 3. Execute as mesmas etapas para callserver_certificate:

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

CVP OAMP (implantação do UCCE)

Como na solução PCCE versão 12.x todos os componentes da solução são controlados pelo SPOG e o OAMP não está instalado, essas etapas são necessárias apenas para uma solução de implantação do UCCE.

Etapa 1. Para excluir os certificados do servidor WSM e OAMP, execute estes comandos:

%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

Digite a senha do armazenamento de chaves quando solicitado.

Etapa 2. Para gerar o certificado WSM, execute este comando:

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

Digite a senha do armazenamento de chaves quando solicitado.

Especifique o FQDN do servidor para a consulta qual é seu nome e sobrenome? e continue com as mesmas etapas como feito com os servidores CVP.

Etapa 3. Execute as mesmas etapas para oamp_certificate:

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

Digite a senha do armazenamento de chaves quando solicitado.

2. Gerar o CSR

Observação: o navegador compatível com RFC5280 requer que o Nome Alternativo do Assunto (SAN) seja incluído em cada certificado. Isso pode ser feito usando o parâmetro ext com SAN ao gerar o CSR.

Nome Alternativo do Assunto

O parâmetro -ext permite que um usuário especifique extensões. O exemplo mostrado adiciona um nome alternativo de requerente (SAN) com o nome de domínio totalmente qualificado (FQDN) do servidor, bem como o host local. Campos SAN adicionais podem ser adicionados como valores separados por vírgula.

Os tipos válidos de SAN são:

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

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

Servidores CVP

Etapa 1. Gere a solicitação de certificado para o alias. Execute este comando e salve-o em um arquivo (por exemplo, wsm_certificate):

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

Digite a senha do armazenamento de chaves quando solicitado.

Etapa 2. Execute as mesmas etapas para vxml_certificate e callserver_certificate:

%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 -

Digite a senha do armazenamento de chaves quando solicitado.

servidor de relatórios CVP

Etapa 1. Gere a solicitação de certificado para o alias. Execute este comando e salve-o em um arquivo (por exemplo, wsmreport_certificate):

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

Digite a senha do armazenamento de chaves quando solicitado.

Etapa 2. Execute as mesmas etapas para o callserver_certificate:

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

Digite a senha do armazenamento de chaves quando solicitado.

CVP OAMP (implantação do UCCE)

Etapa 1. Gere a solicitação de certificado para o alias. Execute este comando e salve-o em um arquivo (por exemplo, oamp_certificate):

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -Ensure to replace "mycvp.mydomain.com" with your OAMP FQDN. Enter the keystore password when prompted.

Etapa 2. Execute as mesmas etapas para oamp_certificate:

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

Digite a senha do armazenamento de chaves quando solicitado.

3. Obter os Certificados Assinados pela CA

Etapa 1. Assine os certificados em uma autoridade de certificação (WSM, Callserver e VXML server para o servidor CVP; WSM e OAMP para o servidor CVP OAMP e WSM e Callserver para o servidor Reporting).

Etapa 2. Baixe os certificados de aplicativo e o certificado raiz da autoridade de certificação.

Etapa 3. Copie o certificado raiz e os certificados assinados pela autoridade de certificação na pasta %CVP_HOME%\conf\security\ de cada servidor.

4. Importar os Certificados Assinados pela CA

Aplique estas etapas a todos os servidores da solução CVP. Somente os certificados para componentes nesse servidor precisam ter o certificado assinado pela autoridade de certificação importado.

Etapa 1. Importe o certificado raiz. Execute este comando:

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

Digite a senha do armazenamento de chaves quando solicitado. No prompt Confiar neste certificado, digite Sim.

Se houver um certificado intermediário, execute este comando:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias intermediate_ca -file

Digite a senha do armazenamento de chaves quando solicitado. No prompt Confiar neste certificado, digite Sim.

Etapa 2. Importe o WSM assinado pela CA para esse certificado de servidor (CVP, Reporting and OAMP). Execute este comando:

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

Digite a senha do armazenamento de chaves quando solicitado. No prompt Confiar neste certificado, digite Sim.

Etapa 3. Nos servidores CVP e nos servidores de relatórios, importe o certificado CA Signed do Callserver. Execute este comando:

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

Digite a senha do armazenamento de chaves quando solicitado. No prompt Confiar neste certificado, digite Sim.

Etapa 4. Nos servidores CVP, importe o certificado assinado da autoridade de certificação do servidor VXML. Execute este comando:

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

Etapa 5. No servidor CVP OAMP (somente para UCCE), importe o certificado CA Signed do servidor OAMP. Execute este comando:

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

Etapa 6. Reinicialize os servidores.

Observação: na implantação do UCCE, certifique-se de adicionar os servidores (Reporting, CVP Server e assim por diante) no CVP OAMP com o FQDN fornecido quando você gerou o CSR.

Servidores VOS

1. Gerar Certificado CSR

Este procedimento explica como gerar o certificado Tomcat CSR a partir de plataformas baseadas no Cisco Voice Operating System (VOS). Esse processo se aplica a todos os aplicativos baseados em VOS, como:

- CUCM
- Finesse
- CUIC \ Live Data (LD) \Identity Server(IDS)
- Conexão em nuvem
- Cisco VVB

Etapa 1. Navegue para a página de administração do sistema operacional Cisco Unified Communications: <u>https://FQDN</u>:<8443 ou 443>/cmplatform.

Etapa 2. Navegue para Segurança > Gerenciamento de certificado e selecione Gerar CSR.

Show - Settings - Security	- Software Upgrades - Services - Help -	
Certificate List		
🙉 Generate SetTaigned 🐴	29load Certificate/Certificate chain	
Certificate List		
Find Certificate List where Ce	rtificate v begins with v	Find Clear Filter 🌵 🚥
		io active query. Please enter your search criteria using the options above.
Generate Self-signed Up	oad Certificate/Certificate chain Generate C	58

Etapa 3. Depois que o certificado CSR for gerado, feche a janela e selecione Download CSR.

Show - Settings - Secu	rity • Software Upgrades •	Services • Help •			
Certificate List					
💽 Generate Sett-signed 🛛	biological Certificate/Certificate of	hain Generate CSR	Download CSR		
Certificate List					
Find Certificate List where	Certificate V begins v	ith 🖂	Find	Clear filter 💠 📟	
		5	o active query. Please	enter your search oriteria using the option	a above.
Generate Self-signed	Upload Certificate/Certificate	chain Generate CS	Download CSR	1	

Etapa 4. Certifique-se de que a finalidade do certificado seja tomcat e clique em Download CSR.

i Download Certificate Signing Request - Mozilla Firefox	-		×
0 A 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			
Certificate Purpose tomcat	×		
Download CSR Close			_
 indicates required item. 			
c			>

Etapa 5. Clique em Save File. O arquivo é salvo na pasta Download.



2. Obter os Certificados Assinados pela CA

Etapa 1. Assinar o certificado tomcat exportado em uma autoridade de certificação.

Etapa 2. Baixe o aplicativo e a raiz certificada da autoridade de certificação.

3. Carregar o Aplicativo e Certificados Raiz

Etapa 1. Navegue para a página de administração do sistema operacional Cisco Unified Communications: <u>https://FQDN</u>:<8443 ou 443>/cmplatform.

Etapa 2. Navegue para Segurança > Gerenciamento de Certificado e selecione Carregar Certificado/Cadeia de Certificado.



Etapa 3. Na janela Carregar certificado/cadeia de certificados, selecione tomcat-trust no campo de finalidade do certificado e carregue o certificado raiz.

Upload Certificate/Certifica	te chain		
Upload 🖳 Close			
Status	stanuida castificata uill distributa it to all sequers in this si	urter	
warning: Oploading a cluster-wide certificate will distribute it to all servers in this cluster			
Upload Certificate/Certifica	ite chain		
Certificate Purpose*	tomcat-trust		
Description(friendly name)			
Upload File	Choose File No file chosen		
Upload Close			

Etapa 4. Carregue um certificado intermediário (se houver) como um tomcat-trust.

Etapa 5. Na janela Upload certificate/Certificate chain, selecione now tomcat no campo Certificate Purpose e carregue o certificado assinado da CA do aplicativo.

Upload Certificate/Certifica	te chain			
Dipload 🖪 Close				
Status Warning: Uploading a clus	ster-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 • indicates required item.				
<		>		

Etapa 6. Reinicialize o servidor.

Verificar

Após reinicializar o servidor, execute estas etapas para verificar a implementação assinada pela CA:

Etapa 1. Abra um navegador da Web e limpe o cache.

Etapa 2. Feche e abra o navegador novamente.

Agora você deve ver o switch de certificado para iniciar o certificado assinado pela CA e a indicação na janela do navegador de que o certificado é autoassinado e, portanto, não confiável, deve desaparecer.

Troubleshooting

Não há etapas para solucionar problemas da implementação dos certificados CA Signed neste guia.

Informações Relacionadas

• Guia de configuração do CVP: Guia de configuração do CVP - Segurança

- Guia de configuração do UCCE: Guia de configuração do UCCE Segurança
- Guia de administração do PCCE: Guia de administração do PCE Segurança
- Certificados UCCE AutoAssinados: <u>Exchange Certificados UCCE AutoAssinados</u>
- Certificados com assinatura automática do PCCE: <u>certificados com assinatura automática</u> <u>do Exchange</u>
- Instalar e migrar para OpenJDK no CCE 12.5(1): migração do CCE OpenJDK
- Instalar e migrar para OpenJDK no CVP 12.5(1): migração do CVP OpenJDK

Suporte Técnico e Documentação - Cisco Systems

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.