Implemente certificados firmados por CA en una solución CCE 12.6

Contenido

Introducción **Prerequisites Requirements** Componentes Utilizados **Background** Procedimiento Servidores basados en Windows de CCE 1. Generar CSR 2. Obtenga los certificados firmados por la CA 3. Cargue los certificados firmados por la CA 4. Enlazar el certificado firmado por la CA a IIS 5. Enlace el certificado firmado por la CA al pórtico de diagnóstico 6. Importe el certificado raíz e intermedio en el almacén de claves Java Solución CVP 1. Generar certificados con FQDN 2. Generar el CSR 3. Obtenga los certificados firmados por la CA 4. Importe los certificados firmados por la CA Servidores VOS 1. Generar certificado CSR 2. Obtenga los certificados firmados por la CA 3. Cargue la aplicación y los certificados raíz Verificación Troubleshoot Información relacionada

Introducción

Este documento describe cómo implementar certificados firmados por la autoridad certificadora (CA) en la solución Cisco Contact Center Enterprise (CCE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Unified Contact Center Enterprise (UCCE), versión 12.6.2
- Paquete Contact Center Enterprise versión 12.6.2
- Customer Voice Portal (CVP) versión 12.6.2
- Navegador de voz virtualizado (VB) de Cisco
- Consola de administración y operaciones de Cisco CVP (OAMP)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Unified Communications Manager (CUCM)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- PCCE 12.6.2
- CVP 12.6.2
- Cisco VB 12.6.2
- Finesss 12.6.2
- CUIC 12.6.2
- Windows 2019

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Background

Los certificados se utilizan para garantizar que la comunicación es segura con la autenticación entre clientes y servidores. Los usuarios pueden comprar certificados de una CA o pueden utilizar certificados autofirmados.

Los certificados autofirmados (como su nombre indica) están firmados por la misma entidad cuya identidad certifican, en lugar de estar firmados por una entidad emisora de certificados. Los certificados autofirmados no se consideran tan seguros como los certificados de CA, pero se utilizan de forma predeterminada en muchas aplicaciones.

En la versión 12.x de la solución Package Contact Center Enterprise (PCCE), todos los componentes de la solución están controlados por un único panel de acceso (SPOG), que se aloja en el servidor principal de la estación de trabajo de administración (AW).

Debido al cumplimiento de la gestión de seguridad (SRC) en la versión PCCE 12.5(1), toda la comunicación entre SPOG y otros componentes de la solución se realiza a través del protocolo HTTP seguro.

Este documento explica en detalle los pasos necesarios para implementar certificados firmados por CA en una solución CCE para una comunicación HTTP segura. Para cualquier otra consideración de seguridad de UCCE, consulte las <u>Pautas de seguridad de UCCE</u>.

Para cualquier comunicación segura de CVP adicional distinta de HTTP seguro, consulte las directrices de seguridad en la Guía de configuración de CVP: <u>Directrices de seguridad de CVP</u>.

Nota: este documento SOLO se aplica a CCE versión 12.6. Consulte la sección de información relacionada para obtener enlaces a otras versiones.

Procedimiento

Servidores basados en Windows de CCE

1. Generar CSR

Este procedimiento explica cómo generar una Solicitud de firma de certificado (CSR) desde el Administrador de Internet Information Services (IIS).

Paso 1. Inicie sesión en Windows y seleccione Panel de control > Herramientas administrativas > Administrador de Internet Information Services (IIS).

Paso 2. En el panel Conexiones, haga clic en el nombre del servidor. Aparecerá el panel Inicio del servidor.



Paso 3. En el área IIS, haga doble clic en Certificados de servidor.



Paso 4. En el panel Acciones, haga clic en Crear solicitud de certificado.

File View Help						
Connections	Server Certificates Use this feature to request and manage certificates that the lifeb server can use with websites configured for SSL Filter: • * * Go • • • Show All Group by:			Actions Import Create Cet Fourie Request Complete Cet Fourie Request. Create Domain Cettificate Control Fold Fourie Centificate		
	Name Cisca ICM Diagnostic Framesc Cisca ICM SSL Cettificate	Issued To PCCLANA.PCCDRCDN.cisco.c., PCCLANA.PCCDRCDN.cisco.c.,	Issued By PCCEANIA.PCCERCE PCCEANIA.PCCERCE	Cruste Self-Signed Certificate Enable Automatic Rebind of Renewed Certificate Help		

Paso 5. En el cuadro de diálogo Solicitar certificado, haga lo siguiente:

Especifique la información necesaria en los campos mostrados y haga clic en Next.

Request Certificate		?	x				
Distinguished Name 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					

En la lista desplegable Proveedor de servicios criptográficos, deje la configuración predeterminada.

En la lista desplegable Longitud de bits, seleccione 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	

Paso 6. Especifique un nombre de archivo para la solicitud de certificado y haga clic en Finalizar.

Request Certificate	?	x
File Name		
Specify the file name for the certificate request. This information can be sent to a certification authority for signing. Specify a file name for the certificate request: PCCEAW.PCCERCDN.cisco.com	f	
Previous Next Finish	Cance	1

2. Obtenga los certificados firmados por la CA

Paso 1. Firmar el certificado en una CA.

Nota: asegúrese de que la plantilla de certificado utilizada por la CA incluya autenticación de cliente y servidor.

Paso 2. Obtenga los certificados firmados por la CA de su autoridad de certificación (raíz, aplicación e intermedio, si los hubiera).

3. Cargue los certificados firmados por la CA

Paso 1. Inicie sesión en Windows y seleccione Panel de control > Herramientas administrativas > Administrador de Internet Information Services (IIS).



Paso 2. En el panel Conexiones, haga clic en el nombre del servidor.

Connections Q,• 🔜 🖄 😥	en en	CEAWA H	ome				
Start Page	Filter		• ¥ 60 -	Show All	Group by:		
	Connection Strings	SMTP E-mail					Î
	Authentic_	Compression	Default	Directory Browsing	Error Pages	Handler Mappings	
	HTTP Redirect	HTTP Respon	ISAPI and CGI Restri	SAPI Filters	Logging	MME Types	
	Modules	Output Caching	8 Request Filtering	Server Certificates	Worker Processes		
	Manageme	1	5			A	
	Configurat	Feature	Shared				3

Paso 3. En el área IIS, haga doble clic en Server Certificates.



Paso 4. En el panel Acciones, haga clic en Completar solicitud de certificado.

File View Help				
Connex-Tions	On Constantion			Actions
Q 🔛 (A) (Q.	Server Ceruica	05		Import
Start Page	Use this feature to request and ma	maps certificates that the Web ser	ver can use with	Cruite Cetificate Report
> S POCCARIA (POCOCOPE) Constraint	websites configured for \$5L			Complete Centificate Report -
	Filter • ?	Create Domain Certificate		
	Name *	Issued To	Issued By	Create Self-Signed Certificate
	Cisca ICM Diagnostic Frames	PCCERMA.PCCORCDN.cisco.c	POCEANIA.POOIRCI	Enable Automatic Rebind of
	Cisco ICM SSL Certificate	PCCLAMAPCCERCIN-cisco-c-	PCCEANA.PCCERCI	Renewed Certificate
				Help
				1

Paso 5. En el cuadro de diálogo Completar solicitud de certificado, complete estos campos:

En el campo Nombre de archivo que contiene la respuesta de la entidad emisora de certificados, haga clic en el botón

Vaya a la ubicación donde se almacena el certificado de aplicación firmado y, a continuación, haga clic en Abrir.

Nota: si se trata de una implementación de CA de nivel 2 y el certificado raíz no está todavía en el almacén de certificados del servidor, la raíz debe cargarse en el almacén de Windows antes de importar el certificado firmado. Consulte este documento si necesita cargar la CA raíz en el almacén de Windows <u>Microsoft - Instalación del certificado raíz de confianza</u>.

En el campo Nombre descriptivo, introduzca el nombre de dominio completo (FQDN) del servidor

o cualquier nombre significativo. Asegúrese de que la lista desplegable Select a certificate store for the new certificate se mantenga como Personal.

Complete Certificate Request	?	×
Specify Certificate Authority Response		
Complete a previously created certificate request by retrieving the file that contains the certificate authority response. Ct/Certificates/PCCEAW/certnew.cer Friendly name: PCCEAWA.pccercdn.cisco.com Select a certificate store for the new certificate Personal v	y's	
OK	Cancel	

Paso 6. Haga clic en Aceptar para cargar el certificado.

Si la carga del certificado se realiza correctamente, el certificado aparece en el panel Certificados de servidor.

🐚 Internet Information Services (15) Manager		_ 0 X	
G S PCCLARA +		₩ × 9 .0 ·	
File View Help			
Connections Q, - El 21 Q, - Ng Start Page > Ng PCCLANA (PCCDRCDN/proceedmin)	Server Certificates Use this feature to request and manage certificates that the Web server can use with websites configured for SSL Filter: • ''' Co Show All Group by:	Actions Import Create Certificate Request Complete Certificate Request. Create Domain Certificate	
	Name Insued To Insued By Coco ICM Diagnostic Framework servi PCOLANA.PCORCENCIESCO PCOLANA.P Coco ICM SR. Certificate PCOLANA.PCORCENCIESCO PCOLANA.P PCOLANA.PCORCENCIESCO PCOLANA.P PCOLANA.pcoercels.cisco.com PCOLECEN.	Create Self-Signed Certificate Enable Automatic Robind of Renewed Certificate @ Holp	

4. Enlazar el certificado firmado por la CA a IIS

Este procedimiento explica cómo enlazar un certificado firmado por una CA en el Administrador de IIS.

Paso 1. Inicie sesión en Windows y seleccione Panel de control > Herramientas administrativas > Administrador de Internet Information Services (IIS).



Paso 2. En el panel Conexiones, elija <nombre_servidor> > Sitios > Sitio Web predeterminado.



Paso 3. En el panel Acciones, haga clic en Enlaces...



Paso 4. Haga clic en el tipo https con el puerto 443, y luego haga clic en Edit....

File View Help		
Connections	Cafault Mah file News	Actions
Q, • 🔄 🖄 🚱. • Vj Stat Page Sta Bindings	Default web site Home	X Explore Edit Permissions
Application Peels Joye Ho http http	it Name Port IP Address Binding Informa Add 10 ' 441 Edit Browse Browse	I dat Site Biodiop: Biodiop: Biodiop: View Applications View Vietnal Directories Manage Website Site Site Site Bioonice 100 (http) Bioonice 100 (http) Bioonice 100 (http)
	Close Close Cutput Request SQL Settings Cutput Request View	Configure Limits W Help
A		er .

Paso 5. En la lista desplegable Certificado SSL, seleccione el certificado con el mismo nombre descriptivo que en el paso anterior.

🕞 internet information Services (15) Manager	- 0 X
Ge	🖬 🖂 🔒 i 🔒 •
File View Help	
Ne View Help	Actions Configure Configu
To Features View	
Testy	٩.

Paso 6. Click OK.

Paso 7. Vaya a Inicio > Ejecutar > services.msc y reinicie el Servicio de administración de IIS.

Q, Services					- 0	x
File Action View	Help					
🔶 🔶 🚾 👘 🖄	i 🔒 📓 🖽 🕨 🔳 🖬 🔟 👘					
() Services (Local)	 Service (Local) 					
	Apache Tomost 9	Name	Description	Status	Statup Type	Let n.
		Q.Hyper V Data Exchange Service	Provides a mechanism to exchange data betwee		Manual (Trip	Los
	Stop the service	Q. Hyper-V Guest Service Interface	Provides an interface for the Hyper-V host to int		Manual (Trip-	Los
	Restart the service	C. Hyper-Y Guest Shutdown Service	Provides a mechanism to shut down the operati		Manual (Trip	Los
		C. Hyper-Y Heatbest Service	Monitors the state of this virtual machine by rep		Manual (Trip	Les
	Osseription	C. Hyper-Y PowerShell Direct Service	Provides a mechanism to manage virtual machi		Manual (Trig.,	Los
	Apache Tomost 80 Server -	Q Hyper-Y Remote Desistop Virtualizatio	Provides a platform for communication betwee		Manual (Trip	Los_
	http://tomcat.apache.org/tomcat/	Q Hyper-V Time Synchronization Service	Synchronizes the system time of this virtual mac		Manual (Trip.,	Los B
		C. Hyper V Volume Shadow Copy Reput	Coordinates the communications that are requir		Manual (Trip.,	100
		15 Admin Service	Enables this server to administer the IS metabas	Renning	Automatic	Los
		CL RI and Ruthill Page Caying Modules	The REECT service heats the Internet Key Excha-	Running	Automatic (T.,	Los
		Contenactive Services Detection	Enables user notification of user input for intera		Disabled	Les
		Q Internet Connection Sharing (ICS)	Provides network address translation, addressin		Disabled	Les
		Q.P Helper	Provides tunnel connectivity using IPv6 transitio	Renning	Automatic	Los
		 Posc Policy Agent 	Internet Protocol security (Poec) supports netw-	Renning	Manual (Trip.,	No
		QuADC Proxy Server service (APS)	KDC Proxy Server service runs on edge servers to		Manual	No
		Q. Renfin for Distributed Transaction C	Coordinates transactions between the Distribute		Manual (Triga-	Ne

5. Enlace el certificado firmado por la CA al pórtico de diagnóstico

Este procedimiento explica cómo enlazar un certificado firmado por CA en el pórtico de diagnóstico.

Paso 1. Abra el símbolo del sistema (Ejecutar como administrador).

Paso 2. Vaya a la carpeta principal de Diagnostic Portico (Pórtico de diagnóstico). Ejecute este

comando:

cd c:\icm\serviceability\diagnostics\bin

Paso 3. Quite el enlace de certificado actual al pórtico de diagnóstico. Ejecute este comando:

DiagFwCertMgr /task:UnbindCert



c:\icm\serviceability\diagnostics\bin>

Paso 4. Abra el certificado firmado y copie el contenido hash (sin espacios) del campo Huella digital.

Nota: Asegúrese de eliminar cualquier carácter oculto del principio o del final del contenido hash. Un editor como Notepad++ puede ayudarle a identificar estos caracteres ocultos.

Certificate		×
General Details Certification Path	1	
Show: <all></all>	¥	
Field Authority Key Identifier CRL Distribution Points Authority Information Access Certificate Template Inform Application Policies Key Usage Thumbprint algorithm Thumbprint	Value ∧ KeyID=03 2f 51 02 27 8c c7 3 [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc [1]Authority Info Access: Acc Template=CC Web Server(1.3 [1]Application Certificate Polic Digital Signature, Key Encipher ≡ sha1 97 93 74 00 99 19 53 d6 4e 0b	
97 93 74 00 99 19 53 96 36 dc 4b cb	d6 4e 0b c5 6e c4 4c bd	
E	dit Properties Copy to File	
	OK	

Paso 5. Ejecute este comando y pegue el contenido hash.

::\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:BindCertFromStore /certhash:97937400991953d64e0bc56ec44cbd963 c4bcb 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 0.0.0.0:7890 completed successfully Found existing registry key for the service Hash of certificate used saved in the service registry ALL TASKS FOR BINDING THE CERTIFICATE WITH HTTP SERVICE COMPLETED SUCCESSFULLY :\icm\serviceability\diagnostics\bin>

Si el enlace del certificado es correcto, muestra el mensaje El enlace del certificado es VÁLIDO.

Paso 6. Valide si el enlace de certificado se realizó correctamente. Ejecute este comando:

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>

Nota: DiagFwCertMgr utiliza el puerto 7890 de forma predeterminada.

Si el enlace del certificado es correcto, muestra el mensaje El enlace del certificado es VÁLIDO.

Paso 7. Reinicie el servicio Marco de diagnóstico. Ejecute estos comandos:

net stop DiagFwSvc net start DiagFwSvc

Si Diagnostic Framework se reinicia correctamente, no aparecerán advertencias de error de certificado cuando se inicie la aplicación.

6. Importe el certificado raíz e intermedio en el almacén de claves Java

Precaución: Antes de comenzar, debe realizar una copia de seguridad del almacén de claves y ejecutar los comandos desde el directorio raíz de Java como administrador.

Paso 1. Conozca la ruta de inicio de java para asegurarse de dónde está alojada la herramienta clave de java. Hay un par de maneras de encontrar la ruta de inicio de Java.

Opción 1: comando CLI: echo %CCE_JAVA_HOME%



Opción 2: Manualmente a través de la configuración avanzada del sistema, como se muestra en la imagen

	el > System and Security > System		5 V	Search Control Panel
ol Panel Home		7		
e Manager	System Properties ×			
te settings	You must be logged on as an Administrator to make most of these changes.	Environment Variables		
nced system settings	Performance	User variables for Administrator		
	Visual effects, processor scheduling, memory usage, and vitual memory	Variable	Value	
	Settings	Path	C:\Users\Administrator\AppData\Local\Microsoft\WindowsA	pps;
	User Profiles	TMP	C:\Users\Administrator\AppData\Local\Temp 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	
		CCE_JAVA_HOME COMPLUS_ProtAPI_ProtilerC	C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot EnableV2Profiler	
	OK Cancel Apply	ComSpec	C:\Windows\system32\cmd.exe	
		COR_PROFILER	AppDynamics.AgentProfiler	
		CORECLR_ENABLE_PROFILI CORECLR_PROFILER	1 AppDynamics.AgentProfiler	
			New	Edit Delete
			E	OK Cancel
so				

Paso 2. Realice una copia de seguridad del archivo cacerts desde las rutas ICM y OpenJDK <directorio de instalación ICM>\ssl\ y %CCE_JAVA_HOME%\lib\security\cacerts. Puede copiarlos en otra ubicación.

Paso 3. Abra una ventana de comandos como Administrador y ejecute estos comandos:

```
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
```

Nota: los certificados específicos necesarios dependen de la CA que utilice para firmar los certificados. En una CA de dos niveles, típica de las CA públicas y más segura que las CA internas, debe importar tanto los certificados raíz como los intermedios. En una CA independiente sin intermediarios, que generalmente se ve en un laboratorio o en una CA interna más simple, solo necesita importar el certificado raíz. Los certificados raíz e intermedios deben importarse a los almacenes de claves ICM y OpenJDK, ya que la CLI del sistema sigue utilizando el almacén de claves OpenJDK.

Solución CVP

1. Generar certificados con FQDN

Este procedimiento explica cómo generar certificados con FQDN para los servicios Web Service Manager (WSM), Voice XML (VXML), Call Server y Operations Management (OAMP).

Nota: Al instalar CVP, el nombre del certificado sólo incluye el nombre del servidor y no el FQDN; por lo tanto, debe volver a generar los certificados.

Precaución: antes de empezar, debe hacer lo siguiente:

1. Abra una ventana de comandos como administrador.

2. Para 12.6.2, para identificar la contraseña del almacén de claves, vaya a la carpeta %CVP_HOME%\bin y ejecute el archivo DecryptKeystoreUtil.bat.

3. Para 12.6.1, para identificar la contraseña del almacén de claves, ejecute el comando more %CVP_HOME%\conf\security.properties.

4. Necesita esta contraseña cuando ejecute los comandos keytool.

5. En el directorio %CVP_HOME%\conf\security\, ejecute el comando copy .keystore backup.keystore.

Servidores CVP

Paso 1. Para eliminar los certificados de servidores CVP, ejecute estos 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

Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 2. Para generar el certificado WSM, ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

Nota: de forma predeterminada, los certificados se generan para dos años. Utilice -valid XXXX para establecer la fecha de caducidad cuando se vuelven a generar los certificados; de lo contrario, los certificados son válidos durante 90 días y deben estar firmados por una CA antes de esta fecha. Para la mayoría de estos certificados, entre 3 y 5 años deben ser un tiempo de validación razonable.

Estas son algunas entradas de validez estándar:

Un año	365

Dos años	730
Tres años	1095
Cuatro años	1460
Cinco años	1895
Diez años	3650

Precaución: a partir de certificados 12.5 deben ser SHA 256, Key Size 2048, y encryption Algorithm RSA, utilice estos parámetros para establecer estos valores: -keyalg RSA y - keysize 2048. Es importante que los comandos del almacén de claves CVP incluyan el parámetro -storetype JCEKS. Si esto no se hace, el certificado, la clave o peor aún el almacén de claves puede dañarse.

Especifique el FQDN del servidor, en la pregunta ¿cuál es su nombre y apellidos?



Complete estas otras preguntas:

¿Cuál es el nombre de la unidad organizativa?

[Desconocido]: <especificar OU>

¿Cuál es el nombre de su organización?

[Desconocido]: <especifique el nombre de la organización>

¿Cuál es el nombre de su ciudad o localidad?

[Desconocido]: <especifique el nombre de la ciudad/localidad>

¿Cuál es el nombre de su estado o provincia?

[Desconocido]: <especifique el nombre del estado o provincia>

¿Cuál es el código de país de dos letras para esta unidad?

[Desconocido]: <especificar código de país de dos letras>

Especifique yes para las dos entradas siguientes.

Paso 3. Realice los mismos pasos para vxml_certificate y 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 informes de CVP

Paso 1. Para eliminar los certificados de WSM y del servidor de informes, ejecute estos 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

Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 2. Para generar el certificado WSM, ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

Especifique el FQDN del servidor para la consulta ¿cuál es su nombre y apellido? y continúe con los mismos pasos que realizó con los servidores CVP.

Paso 3. Realice los mismos pasos para callserver_certificate:

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

CVP OAMP (implementación de UCCE)

Dado que en la versión 12.x de la solución PCCE todos los componentes de la solución están controlados por SPOG y OAMP no está instalado, estos pasos solo son necesarios para una

solución de implementación de UCCE.

Paso 1. Para eliminar los certificados de servidor WSM y OAMP, ejecute estos 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

Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 2. Para generar el certificado WSM, ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

Especifique el FQDN del servidor para la consulta ¿cuál es su nombre y apellido? y continúe con los mismos pasos que realizó con los servidores CVP.

Paso 3. Realice los mismos pasos para oamp_certificate:

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

2. Generar el CSR

Nota: El explorador compatible con RFC5280 requiere que se incluya el nombre alternativo del sujeto (SAN) con cada certificado. Esto se puede lograr utilizando el parámetro -ext con SAN al generar el CSR.

Nombre alternativo del asunto

El parámetro -ext permite al usuario especificar extensiones. En el ejemplo que se muestra se agrega un nombre alternativo de sujeto (SAN) con el nombre de dominio completo (FQDN) del servidor, así como el host local. Los campos SAN adicionales se pueden agregar como valores separados por comas.

Los tipos de SAN válidos son:

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

Por ejemplo:

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

Servidores CVP

Paso 1. Genere la solicitud de certificado para el alias. Ejecute este comando y guárdelo en un archivo (por ejemplo, wsm_certificate):

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 2. Realice los mismos pasos para vxml_certificate y 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 -
```

Introduzca la contraseña del almacén de claves cuando se le solicite.

servidor de informes de CVP

Paso 1. Genere la solicitud de certificado para el alias. Ejecute este comando y guárdelo en un archivo (por ejemplo, wsmreport_certificate):

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 2. Realice los mismos pasos para callserver_certificate:

Introduzca la contraseña del almacén de claves cuando se le solicite.

CVP OAMP (solo implementación de UCCE)

Paso 1. Genere la solicitud de certificado para el alias. Ejecute este comando y guárdelo en un archivo (por ejemplo, wsmoamp_certificate):

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 2. Realice los mismos pasos para oamp_certificate:

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

Introduzca la contraseña del almacén de claves cuando se le solicite.

3. Obtenga los certificados firmados por la CA

Paso 1. Firme los certificados en una CA (servidor WSM, Callserver y VXML para el servidor CVP; WSM y OAMP para el servidor CVP OAMP, y WSM y Callserver para el servidor de informes CVP).

Paso 2. Descargue los certificados de aplicación y el certificado raíz de la autoridad de la CA.

Paso 3. Copie el certificado raíz y los certificados firmados por la CA en la carpeta %CVP_HOME%\conf\security\ de cada servidor.

4. Importe los certificados firmados por la CA

Aplique estos pasos a todos los servidores de la solución CVP. Sólo los certificados de los componentes de ese servidor necesitan importar el certificado firmado por la CA.

Paso 1. Importe el certificado raíz. Ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite. En el mensaje Confiar en este certificado, escriba Sí.

Si hay un certificado intermedio, ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite. En el mensaje Confiar en este certificado, escriba Sí.

Paso 2. Importe el WSM firmado por la CA para ese certificado de servidor (CVP, informes y OAMP). Ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite. En el mensaje Confiar en este certificado, escriba Sí.

Paso 3. En los servidores CVP y los servidores de informes importan el certificado CA de Callserver con firma. Ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite. En el mensaje Confiar en este certificado, escriba Sí.

Paso 4. En los servidores CVP, importe el certificado firmado de CA del servidor VXML. Ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite. En el mensaje Confiar en este certificado, escriba Sí.

Paso 5. En el servidor OAMP de CVP (sólo para UCCE) importe el certificado firmado de CA del servidor OAMP. Ejecute este comando:

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

Introduzca la contraseña del almacén de claves cuando se le solicite. En el mensaje Confiar en este certificado, escriba Sí.

Paso 6. Reinicie los servidores.

Nota: En la implementación de UCCE, asegúrese de agregar los servidores (Informes de CVP, Servidor de CVP, etc.) en CVP OAMP con el FQDN proporcionado al generar el CSR.

Servidores VOS

1. Generar certificado CSR

Este procedimiento explica cómo generar el certificado CSR de Tomcat a partir de plataformas basadas en Cisco Voice Operating System (VOS).

Este proceso se aplica a las aplicaciones basadas en VOS, como:

- Finesse
- CUIC \ Datos en directo (LD) \Identity Server(IDS)
- Conexión a la nube
- VB de Cisco

Paso 1. Vaya a la página de administración del sistema operativo Cisco Unified Communications:https://FQDN :<8443 o 443>/cmplatform.

Paso 2. Navegue hasta Seguridad > Administración de certificados y seleccione Generar CSR.

Show * Settings * Security * Software Upgrades * Services *	Heb +
Certificate List	
🖳 Generate Self-signed 🖓 Upload Certificate/Certificate chain 💽 Ge	nerate CSR
Certificate List	
Find Certificate List where Certificate V begins with V	Find Clear Filter 🌵 🚥
	No active query. Please enter your search criteria using the options above.
Generate Self-signed Upload Certificate/Certificate chain Generate Self-signed Upload Certificate/Certificate chain	nerate CSR

Paso 3. Una vez generado el certificado CSR, cierre la ventana y seleccione Descargar CSR.

Show . Settings . Security . Software Upgrades . Services . Help .	
Certificate List	
💽 Generate Self-signed ing Upload Certificate/Certificate chain 💽 Generate CSR	Counted CSR
Certificate List	
Find Certificate List where Certificate V begins with V	Find Clear Filter 💠 🚥
n n	o active query. Please enter your search orberia using the options above.
Generate Self-signed Upload Certificate/Certificate chain Generate C	SR Download CSR

Paso 4. Asegúrese de que el propósito del certificado es tomcat y haga clic en Descargar CSR.

Download Certificate Signing Request - Mozilla Firefox	-	\times
🛛 🔒 https://10.201.224.234/cmplatform/certificateDownloadNewCsr.do		 Ξ
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 • indicates required item.	<u></u>	
<		>

Paso 5. Haga clic en Guardar archivo. El archivo se guarda en la carpeta Download (Descargar).



- 2. Obtenga los certificados firmados por la CA
- Paso 1. Firmar el certificado de Tomcat exportado en una CA.
- Paso 2. Descargue la aplicación y la raíz certificada de la autoridad de la CA.
- 3. Cargue la aplicación y los certificados raíz

Paso 1. Vaya a la página de administración del sistema operativo Cisco Unified Communications: <u>https://FQDN</u>:<8443 o 443>/cmplatform.

Paso 2. Navegue hasta Seguridad > Administración de certificados y seleccione Cargar certificado/cadena de certificados.



Paso 3. En la ventana Cargar certificado/cadena de certificados, seleccione tomcat-trust en el campo de propósito del certificado y cargue el certificado raíz.

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

Paso 4. Cargue un certificado intermedio (si lo hubiera) como tomcat-trust.

Paso 5. En la ventana Cargar certificado/cadena de certificado, seleccione ahora tomcat en el campo Propósito del certificado y cargue la aplicación Certificado firmado por CA.

Upload Certificate/Certificate/	te chain	
Dipload 🖳 Close		
Status Warning: Uploading a clu Upload Certificate/Certific	ister-wide certificate will distribute it to all servers in this cluster]
Certificate Purpose*	tomcat	
Description(friendly name) Upload File	Self-signed certificate Browse No file selected.	
Upload Close	m.	
<		>

Paso 6. Reinicie el servidor

Verificación

Después de reiniciar el servidor, ejecute estos pasos para verificar la implementación firmada por la CA:

Paso 1. Abra un explorador Web y borre la caché.

Paso 2. Cierre y vuelva a abrir el explorador.

Ahora debe ver el modificador de certificados para iniciar el certificado firmado por la CA y la indicación en la ventana del explorador de que el certificado está autofirmado y, por lo tanto, no es de confianza, debe desaparecer.

Troubleshoot

No hay pasos para solucionar problemas de implementación de certificados firmados por CA en esta guía.

Información Relacionada

• Guía de configuración de CVP - Seguridad

- <u>Guía de seguridad de UCCE</u>
- Guía de administración de PCCE
- <u>Certificados autofirmados de Exchange PCCE PCCE 12.5</u>
- Certificados autofirmados de Exchange UCCE: UCCE 12.5
- Certificados autofirmados de Exchange PCCE PCCE 12.6
- <u>Certificados autofirmados de Exchange UCCE: UCCE 12.6</u>
- Utilidad de intercambio de certificados
- Soporte Técnico y Documentación Cisco Systems

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).