Configuración de la inscripción y renovación automáticas de certificados a través de CAPF Online CA

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Validar la fecha y la hora del servidor Actualizar nombre de equipo del servidor Configurar Plantilla de certificados, usuarios y servicios de AD Configuración de Autenticación IIS y Enlace SSL Configuración de CUCM Verificar certificados IIS Verificar configuración de CUCM Enlaces relacionados

Introducción

En este documento se describe la inscripción y renovación automáticas de certificados mediante la función en línea Certificate Authority Proxy Function (CAPF) para Cisco Unified Communications Manager (CUCM).

Colaboración de Michael Mendoza, ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Communications Manager
- Certificados X.509
- Servidor Windows
- Active Directory (AD) de Windows
- Servicios de Windows Internet Information Server (IIS)
- Autenticación NT (nueva tecnología) LAN Manager (NTLM)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

• CUCM, versión 12.5.1.10000-22

- Windows Server 2012 R2
- IP Phone CP-8865 / Firmware: SIP 12-1-1SR1-4 y 12-5-1SR2.

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.

Antecedentes

Este documento trata la configuración de la función y los recursos relacionados para una investigación adicional.

Validar la fecha y la hora del servidor

Asegúrese de que el servidor de Windows tiene la fecha, hora y zona horaria correctas configuradas, ya que afectan a los tiempos de validez del certificado de la CA (autoridad de certificación) raíz del servidor, así como a los certificados emitidos por él.

Actualizar nombre de equipo del servidor

De forma predeterminada, el nombre del equipo del servidor tiene un nombre aleatorio, como WIN-730K65R6BSK. Lo primero que se debe hacer antes de habilitar los Servicios de dominio de AD es asegurarse de actualizar el nombre de equipo del servidor a lo que desea que sean el nombre de host y el nombre de emisor de la CA raíz del servidor al final de la instalación; de lo contrario, se necesitan muchos pasos adicionales para cambiar esto después de instalar los servicios de AD.

- Vaya a Servidor local, seleccione el nombre del equipo para abrir las Propiedades del sistema
- Seleccione el botón Change y escriba el nuevo nombre de equipo:



• Reinicie el servidor para aplicar los cambios

Configurar

Plantilla de certificados, usuarios y servicios de AD

Habilitar y configurar servicios de Active Directory

• En Administrador del servidor, seleccione la opción **Agregar funciones y características**, seleccione **Instalación basada en funciones o en características** y elija el servidor del grupo (sólo debe haber uno en el grupo) y, a continuación, Servicios de dominio de Active Directory:



- Continúe seleccionando el botón Next y, a continuación, Install
- Seleccione el botón Close después de completar la instalación
- Aparecerá una ficha de advertencia en Administrador del servidor > AD DS con el título Configuración necesaria para los Servicios de dominio de Active Directory; Seleccione el vínculo más y, a continuación, la acción disponible para iniciar el asistente de configuración:



• Siga las indicaciones del asistente de configuración de dominio, agregue un nuevo bosque con el nombre de dominio raíz deseado (usado michamen.com para este laboratorio) y desmarque la casilla DNS cuando esté disponible, defina la contraseña de DSRM (usada *C1sc0123!* para este laboratorio):

in .	Active Directory Domain Services C	onfiguration Wizard	_ _ ×	
Deployment Co	nfiguration		TARGET SERVER	
Deployment Configuration	n Select the deployment operation			
Domain Controller Optio	Add a domain controller to an existing	Add a domain controller to an existing domain		
	Add a new domain to an existing fore	st		
	Add a new forest			
	County the description for this of			
	specity the domain information for this o	peration		
	Root domain name:	michamen.com		

L	Active Directory Domain Se	rvices Configuration Wizard		- • ×
Domain Contro	ller Options		LAB-DC	TARGET SERVER
Deployment Configuration	on Select functional level of the ne	w forest and root domain		
Additional Octions	Forest functional level:	Windows Server 2012 R2	٠	
Paths	Domain functional level:	Windows Server 2012 R2	•	
Review Options	Specify domain controller capal	bilities		
Prerequisites Check	Domain Name System (DNS) server		
	Global Catalog (GC)			
	Read only domain controlle	r (RODC)		
	Type the Directory Services Res	tore Mode (DSRM) password		
	Passwordt	•••••		
	Confirm password:			

- Es necesario especificar un nombre de dominio NetBIOS (se utilizó MICHAMEN1 en este laboratorio).
- Siga el asistente hasta el final. A continuación, el servidor se reinicia para completar la instalación.
- A continuación, deberá especificar el nuevo nombre de dominio la próxima vez que inicie sesión. Por ejemplo, MICHAMEN1\Administrator.

€ Server M	anager • AD DS	· @ I
Dashboard Local Server All Servers	SERVERS All servers 1 total Filter Ø (ii) • (iii) •	•
AD DS	Server Name IPv4 Address Manageability	Last Update

Habilitar y configurar Servicios de Certificate Server

- En Administrador del servidor, seleccione Agregar funciones y características
- Seleccione Servicios de certificados de Active Directory y siga las indicaciones para agregar las características necesarias (todas las características disponibles se seleccionaron de los servicios de rol habilitados para este laboratorio)
- Para servicios de rol, marque Entidad de certificación Inscripción en Web



<u>L</u>	Add Roles and Features Wizard	_ _ X
Select role service	Select the role services to install for Web Server (IIS) Role services	DESTINATION SERVER LAB-DC-ATR/michamen.com
	< Previous Next	> Install Cancel

• Debe aparecer una ficha de advertencia en Administrador del servidor >AD DS con el título Configuración necesaria para los Servicios de certificados de Active Directory; seleccione el vínculo más y, a continuación, la acción disponible:

E Deshtoard	SERVERS Al servers 1 tots				166 *	Ê	
Local Server Al Servers Al Servers	Configuration requ	pred for Active Directory Centificate S P (8) • (8)	enion at UAB-DC-819		Man. ×		
AD DS	Senerhane INARA	International States and American States	Last Epidete not started 205/2019 4211	Windows-Activation () PM Not activated		1.0	
to is		4		All Servers Task Det	alts		Ŀ
		All Servers Tas	k Details and No	otifications			
		All Taolio [1 total					
	panas	All Taolos 1 total	P				

- En el Asistente para configuración posterior a la instalación de AD-CS, desplácese por estos pasos:
- Seleccione las funciones de inscripción en Web Entidad de certificación y Entidad de certificación
- Elija Enterprise CA con opciones:
- CA raíz
- Crear una nueva clave privada
- Usar clave privada: SHA1 con la configuración predeterminada
- Establezca un nombre común para la CA (debe coincidir con el nombre de host del servidor):

8	AD CS Configuration
CA Name	DESTINATION SERVER LAB-DC-RTP.michamen.com
Credentials Role Services	Specify the name of the CA
Setup Type CA Type	Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.
Private Key	Common name for this CA:
CA Name	LAB-DC-RTP
Validity Period	Distinguished name suffice
Certificate Database	DC=michamen,DC=com
Confirmation	Preview of dictionuiched name:
	CN=L48-DC-8TP DC=michamen DC=com

- Establecer validez para 5 años (o más si se desea)
- Seleccione el botón Next en el resto del asistente

Creación de plantillas de certificados para CiscoRA

- Abra MMC. Seleccione el logotipo de inicio de Windows y escriba mmc en Ejecutar
- Abra una ventana MMC y agregue los siguientes complementos (utilizados en diferentes puntos de la configuración) y, a continuación, seleccione **Aceptar**:



- Seleccione File > Save y guarde esta sesión de consola en el escritorio para acceder de nuevo rápidamente
- En los complementos, seleccione Plantillas de certificado
- Cree o clone una plantilla (preferiblemente la plantilla "*Entidad emisora de certificados raíz*", si está disponible) y asígnele el nombre CiscoRA

Cons Cons	sole1 - [Console Root\Certificate T	emplates (LAB-DC-
 File Action View Favorites Window Help 		
Console Root	Template Display Name	Schema Version
Active Directory Domains and Trusts	Administrator	1
Active Directory Users and Computers	Authenticated Session	1
Certification Authority (Local)	Basic EFS	1
Certricate i empirates [LAR-DC-KTP.michamen.com] With internet information Services (IIS) Manager	CA Exchan CEP Encryp Code Signi Reenroll All Certific	ate Holders

- Modifique la plantilla. Haga clic con el botón derecho del ratón y seleccione Propiedades
- Seleccione la pestaña **General** y establezca el período de validez en 20 años (u otro valor si lo desea). En esta ficha, asegúrese de que los valores "nombre para mostrar" y "nombre" de la plantilla coinciden

CiscoRA Properties							
Subject Name Issuance Requirements							
Superseded Templates			Extensions	nsions Security Se			
General	General Compatibility Request Handling Cryptography Key Attestation						
Templal	e display name:						
CiscoR	A						
Templa CiscoR Validity :	Template name: CiscoRA Validity period: years v 10 days v						
Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory							
	OK		Cancel	Apply	Help		

• Seleccione la ficha **Extensiones**, resalte **Directivas de aplicación** y, a continuación, seleccione **Editar**



- Elimine las directivas que se muestran en la ventana que aparece
- Seleccione la pestaña Nombre del asunto y el botón de opción Aprovisionar en solicitud
- Seleccione la ficha **Seguridad** y conceda todos los permisos para todos los grupos o nombres de usuario que se muestran

CiscoRA Properties ? X
General Compatibility Request Handling Cryptography Key Attestation Subject Name Issuance Requirements Superseded Templates Extensions Security Server
Group or user names:
Administrator Administrator Administrator Administrator Administrator Adminis (MICHAMEN1\Domain Admins) Enterprise Adminis (MICHAMEN1\Enterprise Adminis)
Add Remove Permissions for Authenticated Users Allow Deny
Full Control
Read 🗹 🗌
Write 🔽 🗌
Enrol 🗹 🗌
Autoenroll For special permissions or advanced settings, click Advanced
OK Cancel Apply Help

Hacer que la plantilla de certificado esté disponible para su emisión

- En los complementos MMC, seleccione **Entidad emisora de certificados** y expanda el árbol de carpetas para localizar la carpeta **Plantillas de certificados**
- Haga clic con el botón secundario en el espacio en blanco del marco que contiene Nombre y Propósito esperado
- Seleccione la plantilla New y Certificate para emitir
- Seleccione la plantilla de CiscoRA recién creada y editada



Creación de cuenta CiscoRA de Active Directory

- Vaya a los complementos MMC y seleccione Usuarios y equipos de Active Directory
- Seleccione la carpeta Users en el árbol del panel del extremo izquierdo
- Haga clic con el botón secundario en el espacio en blanco del marco que contiene Nombre, Tipo y
 Descripción
- Seleccione Nuevo y Usuario
- Cree la cuenta CiscoRA con nombre de usuario/contraseña (*ciscora/Cisco123* se utilizó para este laboratorio) y seleccione la casilla de verificación Password never expires cuando se muestre

	• 📅 🕏 ३ ३ ३ ४ ४ ४ 🖻 ३	
Console Root	Name 8. Administration	Type
Active Directory Uten and Computers (LAB-D) Sevel Queries Signichamac.com	Reveal RODC Password	Security Gro User Security Gro
p 🛄 Builtin p 🛄 Computers	E Crocol A	User Security Gro
Domain Controllers PareignSecurityPrincipals Managed Service Accounts	R Denied RODC Password R Drukdmins R Drukdmins	Security Gro Security Gro Security Gro
 Dien Di Cattoria babaia dana 	SR Domain Admins	Security Gro

IIS Configuración de Autenticación y Enlace SSL

Habilitar NTLM Autenticación

- Vaya a los complementos MMC y, en el complemento Administrador de Internet Information Services (IIS), seleccione el nombre del servidor
- La lista de funciones se muestra en el siguiente fotograma. Haga doble clic en el icono de la función Authentication



 Resalte Autenticación de Windows y en el marco Acciones (panel derecho) seleccione la opción Habilitar

● ● ▲ LAB-DC-RTP →				
Connections Q.•	Authentication Group by: No Grouping			Actions Enable Help
Application Pools P- Sites	Name Anonymous Authentication ASP.NET Impersonation Windows Authentication	Status Enabled Disabled Disabled	Response Type HTTP 401 Challenge	

• El panel Acciones muestra la opción **Configuración avanzada**; selecciónela y desactive **Habilitar** autenticación en modo kernel



• Seleccione Providers y ponga en orden NTML y, a continuación, Negotiate.

Connections	Authentication			Alerts
0, • 🔛 1 🖄 1 🚱.	Authentication			A Click here to learn how
	Group by: No Grouping .	Configure Extended Protection.		
Application Pools	Name *	Status	Response Type	Actions
p- 🖉 Stei	Anonymous Authentication ASP.NET Impersonation	Enabled Disabled		Disable
	Windows Authentication	Enabled	HTTP 401 Challenge	Advanced Settings
	Enabled Providers: NTLM Negotiate Negotiate:Kerberos		Move Up Move Down Remove	U Hop
	Select a provider from the list o to add it to the enabled provide Available Providers:	f available provide os.	v Add	

Generar el certificado de identidad para el servidor Web

Si todavía no es el caso, debe generar un certificado y un certificado de identidad para el servicio Web firmado por la CA porque CiscoRA no puede conectarse a él si el certificado del servidor Web es de firma automática:

• Seleccione el servidor Web en el **complemento IIS** y haga doble clic en el icono de la función **Certificados de servidor**:



• De forma predeterminada, puede ver un certificado enumerado allí: el certificado de CA raíz autofirmado. En el menú Acciones, seleccione la opción Crear certificado de dominio. Ingrese los valores en el asistente de configuración para crear su nuevo certificado. Asegúrese de que el nombre común es un FQDN (nombre de dominio completamente calificado) que se pueda resolver y, a continuación, seleccione Siguiente:



• Seleccione el certificado de la CA raíz para que sea el emisor y seleccione Finalizar:

Create Certificate	?	x
Online Certification Authority		
Specify the certification authority within your domain that will sign the certificate. A friendly name is required and should be easy to remember. Specify Online Certification Authority:		
LAB-DC-RTP\LAB-DC-RTP.michamen.com Select.		
Example: CertificateAuthorityName\ServerName		
Friendly name:		
Web Cert issued by LAB-DC-RTP		
Previous Next Finish C	ancel	

• Puede ver ambos, el certificado de CA y el certificado de identidad del servidor Web:



Enlace SSL de servidor web

• Seleccione un sitio en la vista de árbol (puede utilizar el sitio Web predeterminado o hacerlo más granular para sitios específicos) y seleccione **Enlaces** en el panel Acciones. De este modo, aparece el editor de enlaces que permite crear, editar y eliminar enlaces para el sitio Web. Seleccione **Agregar** para agregar su nuevo enlace SSL al sitio.



• La configuración predeterminada para un nuevo enlace se establece en HTTP en el puerto 80. Seleccione **https** en la lista desplegable **Type**. Seleccione el certificado autofirmado que creó en la sección anterior de la lista desplegable **Certificado SSL** y luego seleccione **Aceptar**.

			Site	Bindings		? X
Type http	Host Name	Port 80	IP Address	Binding Informa		Add Edit
			Add Site Bi	nding	? X	emove
He He	pe: Ips v st name: Require Server Nar	All Unassi	gned	Port: v 443		
SS	L certificate: eb Cert issued by L	AB-DC-RTP		✓ Select	View	Close
LA	it selected to Cert issued by L B-DC-RTP	AB-DC-RTP		ок	Cancel	_

• Ahora tiene un nuevo enlace SSL en su sitio y todo lo que queda es verificar que funciona seleccionando la opción **Browse *:443 (https)** del menú y asegúrese de que la página Web de IIS predeterminada utiliza HTTPS:

Site Bindings				?	
Type	Host Name	Port	IP Address	Binding Informa	Add
https		443	•		Edit
					Bemove
					Browse



• Recuerde reiniciar el servicio IIS después de los cambios de configuración. Utilice la opción **Reiniciar** del panel Acciones.

Configuración de CUCM

 Vaya a la página web de AD CS (<u>https://YOUR_SERVER_FQDN/certsrv/</u>) y descargue el certificado de CA



Navegue hasta Seguridad > Administración de certificados desde la página Administración del SO y seleccione el botón Cargar certificado/cadena de certificado para cargar el certificado de CA con el propósito establecido en CAPF-trust.

Upload Certificate/Certificate chain						
Upload 🖳 Close						
Status Warning: Uploading a clu	uster-wide certificate will distribute it to a					
Upload Certificate/Certific Certificate Purpose* Description(friendly name) Upload File	CAPF-trust Browse LAB-DC-RTP_CA.cer					
Upload Close						

... En este punto, también es buena idea cargar ese mismo certificado de CA como *CallManager-trust* porque es necesario si el cifrado de señalización segura está habilitado (o se habilitará) para los terminales; lo que es probable si el clúster está en modo mixto.

- Vaya a **Sistema > Parámetros de servicio.** Seleccione el servidor del Publicador de Unified CM en el campo del servidor y **Cisco Certificate Authority Proxy Function** en el campo Servicio
- Establezca el valor de Emisor de certificado en Terminal en CA en línea e introduzca los valores para los campos Parámetros de CA en línea. Asegúrese de utilizar el FQDN del servidor Web, el nombre de la plantilla de certificado creada anteriormente (CiscoRA), el tipo de CA como CA de Microsoft y las credenciales de la cuenta de usuario de CiscoRA creada anteriormente

Service Parameter Configuration						
Save 🧬 Set to Default						
Select Server and Service						
Server* cucm125pubCUCM Voice/Video (Active) ~						
Service* Cisco Certificate Authority Proxy Function (Active) 🗸						
All parameters apply only to the current server except parameters that are in the cluster-wide group(s).						
Cisco Certificate Authority Proxy Function (Active) Parameters	s on server cucm125pubCUCM Voice/Video (Activ					
Parameter Name	Parameter Value					
Certificate Issuer to Endpoint *	Online CA					
<u>Certificate Issuer to Endpoint</u> * <u>Duration Of Certificate Validity (in days)</u> *	Online CA 1825					
Certificate Issuer to Endpoint * Duration Of Certificate Validity (in days) * Key Size *	Online CA 1825 1024					
Certificate Issuer to Endpoint * Duration Of Certificate Validity (in days) * Key Size * Maximum Allowable Time For Key Generation *	Online CA 1825 1024 30					
Certificate Issuer to Endpoint * Duration Of Certificate Validity (in days) * Key Size * Maximum Allowable Time For Key Generation * Maximum Allowable Attempts for Key Generation *	Online CA 1825 1024 30 3					
Certificate Issuer to Endpoint.* Duration Of Certificate Validity (in days).* Key Size.* Maximum Allowable Time For Key Generation.* Maximum Allowable Attempts for Key Generation.* Conline CA Parameters	Online CA 1825 1024 30 3					
Certificate Issuer to Endpoint.* Duration Of Certificate Validity (in days).* Key Size.* Maximum Allowable Time For Key Generation.* Maximum Allowable Attempts for Key Generation.* Online CA Parameters Online CA Hostname	Online CA 1825 1024 30 3 lab-dc-iis.michamen.com					
Certificate Issuer to Endpoint * Duration Of Certificate Validity (in days) * Key Size * Maximum Allowable Time For Key Generation * Maximum Allowable Attempts for Key Generation * Online CA Parameters Online CA Hostname Online CA Port	Online CA 1825 1024 30 3 Iab-dc-iis.michamen.com 443					
Certificate Issuer to Endpoint.* Duration Of Certificate Validity (in days).* Key Size.* Maximum Allowable Time For Key Generation.* Maximum Allowable Attempts for Key Generation.* Online CA Parameters Online CA Hostname Online CA Port Online CA Template	Online CA 1825 1024 30 3 Iab-dc-iis.michamen.com 443 CiscoRA					
Certificate Issuer to Endpoint.* Duration Of Certificate Validity (in days).* Key Size.* Maximum Allowable Time For Key Generation.* Maximum Allowable Attempts for Key Generation.* Online CA Parameters Online CA Hostname Online CA Port Online CA Template Online CA Type.*	Online CA 1825 1024 30 3 Iab-dc-iis.michamen.com 443 CiscoRA Microsoft CA					
Certificate Issuer to Endpoint.* Duration Of Certificate Validity (in days).* Key Size.* Maximum Allowable Time For Key Generation.* Maximum Allowable Attempts for Key Generation.* Online CA Parameters Online CA Hostname Online CA Port Online CA Template Online CA Type.* Online CA Username	Online CA 1825 1024 30 3 Iab-dc-iis.michamen.com 443 CiscoRA Microsoft CA ••••••					

Una ventana emergente le informa de que es necesario reiniciar el servicio CAPF. Pero primero, active Cisco Certificate Enrollment Service a través de Cisco Unified Serviceability > Tools > Service Activation, seleccione el publicador en el campo Server y marque la casilla de verificación Cisco Certificate Enrollment Service, y luego seleccione el botón Save:



Verificación

Verificar certificados IIS

• Desde un explorador Web en un PC con conectividad al servidor (preferiblemente en la misma red que el publicador de CUCM), navegue hasta la dirección URL:

https://YOUR_SERVER_FQDN/certsrv/

• Se muestra la alerta de certificado no fiable. Agregue la excepción y compruebe el certificado. Asegúrese de que coincide con el FQDN esperado:



• Después de aceptar la excepción, debe autenticarse; en este punto, debe utilizar las credenciales configuradas para la cuenta CiscoRA anteriormente:

0	
https://lab-dc-iis.michamen.com is requesting your username a	nd password.
User Name: ciscora	
Password:	
OK Cancel	

• Después de la autenticación, debe poder ver la página de bienvenida de AD CS (Servicios de certificados de Active Directory):



Verificar configuración de CUCM

Realice los pasos que sigue normalmente para instalar un certificado LSC en uno de los teléfonos.

- Paso 1. Abra la página CallManager Administration, Device y luego Phone
- Paso 2. Seleccione el botón Find para mostrar los teléfonos
- Paso 3. Seleccione el teléfono en el que desea instalar el LSC
- Paso 4. Desplácese hasta Información de la función proxy de la entidad de certificación (CAPF)
- Paso 5. Seleccione la opción Instalar/Actualizar en la operación de certificado.
- Paso 6. Seleccione el modo de autenticación. (By Null String is fine for test purposes)

Paso 7. Desplácese hasta la parte superior de la página y seleccione save y Apply Config para el teléfono.

Paso 8. Después de que el teléfono se reinicie y vuelva a registrarse, utilice el filtro Estado de LSC para confirmar que el LSC se ha instalado correctamente.

- En el servidor de AD, abra MMC y expanda el complemento Entidad de certificación para seleccionar la carpeta Certificados emitidos
- La entrada del teléfono se muestra en la vista de resumen. Estos son algunos de los detalles que se muestran:
 - ID de solicitud: número de secuencia único
 - Nombre del solicitante: se debe mostrar el nombre de usuario de la cuenta CiscoRA configurada
 - Plantilla de certificado: debe mostrarse el nombre de la plantilla de CiscoRA creada
 - Nombre común emitido: se debe mostrar el modelo del teléfono anexado al nombre del dispositivo
 - Fecha en Vigor del Certificado y Fecha de Vencimiento del Certificado

Console Root	Request ID	Requester Name	Binary Certificate	Certificate Template	Issued Common Name
Active Directory Domains and Tru	2	MICHAMEN1\Administrator	BEGIN CERTI	Web Server (WebSer	LAB-DC-IIS.michamen
Active Directory Users and Compu	3	MICHAMEN1\LAB-DC-RTP\$	BEGIN CERTI	Domain Controller (LAB-DC-RTP.michame
A in Certification Authority (Local)	-4	MICHAMEN1\ciscora	BEGIN CERTI	CiscoRA (1.3.6.1.4.1.3	CP-8865-SEP74A02FC0
a 🚽 LAB-DC-RTP	-				
Revoked Certificates					
Issued Certificates					
Pending Requests					
Failed Requests					
Certificate Templates					

Enlaces relacionados

- Troubleshooting de CAPF Online CA
- <u>Soporte Técnico y Documentación Cisco Systems</u>

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).