Configurazione della registrazione e del rinnovo automatici dei certificati tramite la CA CAPF Online

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Convalida la data e l'ora del server Aggiorna nome computer server Configurazione Servizi AD, utente e modello di certificato Configurazione autenticazione IIS e binding SSL Configurazione CUCM Verifica Verifica certificati IIS Verifica configurazione CUCM Collegamenti correlati

Introduzione

In questo documento viene descritta la registrazione e il rinnovo automatici dei certificati tramite la funzionalità online CAPF (Certificate Authority Proxy Function) per Cisco Unified Communications Manager (CUCM).

Contributo di Michael Mendoza, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Unified Communications Manager
- Certificati X.509
- Windows Server
- Windows Active Directory (AD)
- IIS (Windows Internet Information Services)
- Autenticazione NT (New Technology) LAN Manager (NTLM)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

• CUCM versione 12.5.1.10000-22

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento descrive la configurazione della funzione e le risorse correlate per ulteriori ricerche.

Convalida la data e l'ora del server

Verificare che nel server Windows siano configurati la data, l'ora e il fuso orario corretti in quanto influiscono sui tempi di validità del certificato CA radice (Certification Authority) del server e dei certificati da esso rilasciati.

Aggiorna nome computer server

Per impostazione predefinita, il nome del computer del server è casuale, ad esempio WIN-730K65R6BSK. Prima di abilitare Servizi di dominio Active Directory, è necessario innanzitutto verificare che il nome del computer del server venga aggiornato in base al nome host e al nome autorità emittente della CA radice del server entro la fine dell'installazione. In caso contrario, è necessario eseguire molti passaggi aggiuntivi per modificare questa impostazione dopo l'installazione dei servizi Active Directory.

- Passare a Server locale, selezionare il nome del computer per aprire Proprietà del sistema
- Selezionare il pulsante Cambia e immettere il nuovo nome del computer:



• Riavviare il server per applicare le modifiche

Configurazione

Servizi AD, utente e modello di certificato

Abilitare e configurare i servizi Active Directory

• In Server Manager selezionare l'opzione **Aggiungi ruoli e funzionalità**, selezionare l'**installazione basata su ruoli o su funzionalità** e scegliere il server dal pool (è sufficiente che ne sia presente uno solo nel pool), quindi Servizi di dominio Active Directory:



- Continuare a selezionare il pulsante Next (Avanti), quindi Install (Installa)
- Selezionare il pulsante Chiudi al termine dell'installazione
- In Server Manager > Servizi di dominio Active Directory viene visualizzata una scheda di avviso con il titolo Configurazione richiesta per Servizi di dominio Active Directory. Selezionare altro collegamento, quindi scegliere un'azione disponibile per avviare l'installazione guidata:

Dashboard	All servers 1 tota		T4545 *	
Al Servers AD DS	Filter	P (8 • (8 •	annanz iller x	
File and Storage Services	· · ·	All Serve	s Task Details	
	All Serve	ers Task Details and Notificati	ons	
	All Serve Al Taola 1 tota Filter	ers Task Details and Notificati	ons	(

• Seguire le istruzioni della procedura guidata per l'installazione del dominio, aggiungere una nuova foresta con il nome di dominio radice desiderato (utilizzato michamen.com per questa esercitazione) e deselezionare la casella DNS quando disponibile, definire la password DSRM (utilizzata *C1sc0123!* per questa esercitazione):

2	Active Directory Domain Services Config	uration Wizard 📃 🗖 🗙
Deployment Cor	figuration	TARGET SERVER LAB-DC-RTP
Deployment Configuration Domain Controller Option DNS Options Additional Options	Select the deployment operation Add a domain controller to an existing dom. Add a new domain to an existing forest Add a new forest	sin
Paths Review Options Prerequisites Check	Specify the domain information for this operation Root domain name: michae	m men.com

Options		LAB-DO	TARGET SERVER
Select functional level of the new forest a	and root domain		
Forest functional level:	Windows Server 2012 R2	٣	
Domain functional level:	Windows Server 2012 R2	•	
Specify domain controller capabilities Domain Name System (DNS) server Global Catalog (GC) Read only domain controller (RODC) Type the Directory Services Restore Mod Password: Confirm password:	e (DSRM) password		
	Options Select functional level of the new forest a Forest functional level: Domain functional level: Specify domain controller capabilities Domain Name System (DNS) server Global Catalog (IGC) Read only domain controller (RODC) Type the Directory Services Restore Mod Password: Confirm password:	Options Select functional level of the new forest and root domain Forest functional level: Windows Server 2012 R2 Domain functional level: Windows Server 2012 R2 Specify domain controller capabilities Windows Server 2012 R2 Specify domain controller capabilities Image: Constant Controller Chapabilities Image: Constant Controller Chapabilities Image: Constant Constant Controller Chapabilities Image: Constant Constant Controller Chapabilities Image: Constant	Options LAB-DC Select functional level of the new forest and root domain Forest functional level: Windows Server 2012 R2 * Domain functional level: Windows Server 2012 R2 * Specify domain controller capabilities Domain Name System (DNS) server Ø Global Catalog (GC) Rad only domain controller (RODC) Type the Directory Services Restore Mode (DSRM) password Password: Confirm password: ************************************

- È necessario specificare un nome di dominio NetBIOS (utilizzato da MICHAMEN1 in questa esercitazione).
- Seguire la procedura guidata fino al completamento. Il server viene quindi riavviato per completare l'installazione.
- Quando è necessario specificare il nuovo nome di dominio al prossimo accesso. Ad esempio MICHAMEN1\Administrator.



Abilitare e configurare Servizi certificati

- In Server Manager selezionare Aggiungi ruoli e funzionalità
- Selezionare Servizi certificati Active Directory e seguire le istruzioni per aggiungere le funzionalità necessarie (tutte le funzionalità disponibili sono state selezionate dai servizi ruolo abilitati per questa esercitazione)
- Per i servizi ruolo, selezionare Registrazione Web Autorità di certificazione





• In Server Manager >Servizi di dominio Active Directory deve essere visualizzata una scheda di avviso con il titolo Configurazione richiesta per Servizi certificati Active Directory. Selezionare il collegamento altro e quindi l'azione disponibile:

Configuration required for an Name DVE Address ADC ADP 14.44.31.353	e the Active Directory Certificate So P (8) • (8) S Menageability	Last Spoke	Wedges Actuation	900. ×		
and and the second	a Manapability	Last Update	Windows Activation			
	8 Online - Performance counters	NUMBER 200/2019 4211	00 PM Not activated		ан.	
	All Servers Tas At Tails (1 total	k Details and N	All Servers Task De otifications	tels		-
NTS ents 0 total	Filter Status - Task Name	P (8 •	® • Menage	Action		Notes
N	FS nb:10 total	All Table Victors 1 603 All Table (1 find Filter Butter Table Kame All Table (1 filter Butter Table Kame	All Section 2 Statistics Certainst and the section 2 Statistics and t	All Table 11 tool All Table 11 tool	All Table 1 food Add And Ad	Article 1 total A

- Nella Configurazione guidata post-installazione di AD-CS passare ai passaggi seguenti:
- Selezionare i ruoli di registrazione Web Autorità di certificazione e Autorità di certificazione
- Scegliere CA Enterprise con le opzioni seguenti:
- CA radice
- Crea una nuova chiave privata
- Usa chiave privata SHA1 con impostazioni predefinite
- Impostare un nome comune per la CA (deve corrispondere al nome host del server):

L	AD CS Configuration	- • ×
CA Name	DE LA8-DC-	STINATION SERVER RTRmichamen.com
Credentials Role Services Setup Type CA Type Private Key	Specify the name of the CA Type a common name to identify this certification authority (CA). This name is certificates issued by the CA. Distinguished name suffix values are automatically be modified. Common name for this CA:	added to all y generated but can
Cryptography	LA8-DC-RTP	
Ca reame Validity Period Certificate Database Confirmation Progress Results	Distinguished name suffic: DC=michamen,DC=com Preview of distinguished name: CN=LA8-DC-RTP,DC=michamen,DC=com	

- Impostare la validità per 5 anni (o più, se desiderato)
- Selezionare il pulsante Avanti nel resto della procedura guidata

Creazione di modelli di certificato per CiscoRA

- Aprire MMC. Selezionare il logo di avvio di Windows e digitare mmc da Esegui
- Aprire una finestra di MMC e aggiungere i seguenti snap-in (utilizzati in punti diversi della configurazione), quindi selezionare **OK**:

.....

x

New			c	trl+N
Open			c	trl+O
Save			0	Ctrl+S 4
Save As				4
Add/Rem	ove Sna	ip-in	C	tri+M
Options				2
Options				
			Add	d or Remove Snap-

ap-in	Vendor	~		Console Root	Edit Extensions
Active Directory Do	Microsoft Cor			Active Directory Domains and True	
Active Directory Site	Microsoft Cor			Active Directory Users and Compu-	Remove
Active Directory Use	Microsoft Cor	-		Certification Authority (Local)	
ActiveX Control	Microsoft Cor			Certificate Templates (LAB-DC.mic	Move Up
ADSI Edit	Microsoft Cor			Internet Information Services (IIS)	
Authorization Manager	Microsoft Cor				Move Down
Certificate Templates	Microsoft Cor		Add >		
Certificates	Microsoft Cor				
Certification Authority	Microsoft Cor				
Component Services	Microsoft Cor				
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor				
Disk Management	Microsoft and				
DNS	Microsoft Cor	×		< 111 >	Advanced
ription:					
can use the Active Dire	ctory Domains and	To	sts snap-in to m	anage Active Directory domains and trus	te.
				anage recerc an even y annun a na a a	

- Selezionare File > Salva e salvare la sessione della console sul desktop per un rapido riaccesso
- Dagli snap-in, selezionare Modelli di certificato
- Creare o clonare un modello (preferibilmente il modello "*Root Certification Authority*", se disponibile) e denominarlo CiscoRA



- Modificare il modello. Fare clic con il pulsante destro del mouse e selezionare Proprietà
- Selezionare la scheda **Generale** e impostare il periodo di validità su 20 anni (o su un altro valore se desiderato). In questa scheda, assicurarsi che i valori di "nome visualizzato" e "nome" del modello corrispondano

	Cisc	oRA Propert	ies	? X
	Subject Name	lss	ance Require	ments
Supers	eded Templates	Extensions	Security	Server
General	Compatibility Requ	est Handling C	ryptography	Key Attestation
Templat	e display name:			
CiscoR	A			
Templat CiscoR Validity (e name: A seriod: years v	Renewal pe	riod: ys ❤	
<u>Р</u> иы 0	sh certificate in Active to not automatically re irrectory	 Directory enroll if a duplication 	e certificate ex	ists in Active
	ОК	Cancel	Apply	Help

• Selezionare la scheda Estensioni, evidenziare Criteri di applicazione e quindi selezionare Modifica



- Rimuovere tutti i criteri visualizzati nella finestra visualizzata
- Selezionare la scheda Nome soggetto e selezionare il pulsante di opzione Fornitura in richiesta
- Selezionare la scheda **Protezione** e concedere tutte le autorizzazioni per tutti i gruppi/nomi utente visualizzati

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

Rendere il modello di certificato disponibile per il rilascio

- Negli snap-in di MMC selezionare Autorità di certificazione ed espandere la struttura di cartelle per individuare la cartella Modelli di certificato
- Fare clic con il pulsante destro del mouse nello spazio vuoto della cornice contenente Nome e Scopo designato
- Selezionare Nuovo e Modello di certificato da rilasciare
- Selezionare il modello CiscoRA appena creato e modificato



Creazione account CiscoRA Active Directory

- Passare agli snap-in di MMC e selezionare Utenti e computer di Active Directory
- Selezionare la cartella Users nella struttura nel riquadro all'estrema sinistra
- Fare clic con il pulsante destro del mouse nello spazio vuoto della cornice contenente Nome, Tipo e Descrizione
- Seleziona nuovo e utente
- Creare l'account CiscoRA con nome utente/password (*ciscora/Cisco123* è stato utilizzato per questa esercitazione) e selezionare la casella di controllo **Nessuna scadenza password** quando viene visualizzata

	• 🔄 🕏 ३. ११ म 💷 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	Cher 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 Configurazione autenticazione e binding SSL

Abilita NTLM Autenticazione

- Passare agli snap-in di MMC e selezionare il nome del server nello snap-in Gestione Internet Information Services (IIS)
- L'elenco delle funzioni viene visualizzato nel fotogramma successivo. Fare doppio clic sull'icona della funzione di **autenticazione**



• Evidenziare Autenticazione di Windows e nel riquadro Azioni (riquadro di destra) selezionare l'opzione Abilita

(e) (i) LAB-DC-RTP →				
Connections Q, •	Authentication	Actions Enable Help		
	Name Anonymous Authentication ASP.NET Impersonation Windows Authentication	Status Enabled Disabled Disabled	Response Type HTTP 401 Challenge	

• Nel riquadro Azioni viene visualizzata l'opzione **Impostazioni avanzate**; selezionarla e deselezionare **Abilita autenticazione in modalità kernel**



• Selezionare Provider e mettere in ordine NTML quindi Negozia.

Connections 0. • 1 12 19. Start Page 3 Start Page 3 St	Muthentication			Alerts
	Group by: No Grouping .	configure Extended Protection.		
	Name *	Status	Response Type	Actions
þ- 💰 Sites	Anonymous Authentication ASP.NET Impersonation	Enabled		Disable
	Windows Authentication	Enabled	HTTP 401 Challenge	Advanced Settings
	Enabled Providers: Netton Negotiste Negotiste Kerberos Select a provider from the list o to add it to the enabled provide Available Providers:	f available provide	Move Up Move Down Remove rs and click Add	€ Hep

Genera il certificato di identità per il server Web

In caso contrario, è necessario generare un certificato di identità per il servizio Web firmato dalla CA perché CiscoRA non è in grado di connettersi a tale servizio se il certificato del server Web è autofirmato:

• Selezionare il server Web dallo **snap-in IIS** e fare doppio clic sull'icona della funzionalità **Certificati** server:



• Per impostazione predefinita, nell'elenco è presente un certificato, ovvero il certificato CA radice autofirmato. Dal menu **Azioni** selezionare l'opzione **Crea certificato di dominio**. Immettere i valori nella configurazione guidata per creare il nuovo certificato. Verificare che il nome comune sia un nome di dominio completo risolvibile, quindi selezionare **Avanti**:



• Selezionare il certificato della CA radice come autorità di certificazione e scegliere Fine:

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

• È possibile visualizzare sia il certificato CA che il certificato di identità del server Web:



Associazione SSL server Web

• Selezionare un sito nella visualizzazione struttura (è possibile utilizzare il sito Web predefinito o renderlo più granulare per siti specifici) e selezionare **Associazioni** dal riquadro Azioni. Verrà visualizzato l'editor delle associazioni che consente di creare, modificare ed eliminare associazioni per il sito Web. Per aggiungere il nuovo binding SSL al sito, selezionare **Add** (Aggiungi).



• Le impostazioni predefinite per una nuova associazione sono impostate su HTTP sulla porta 80. Selezionare **https** dall'elenco a discesa **Type**. Selezionare il certificato autofirmato creato nella sezione precedente dall'elenco a discesa **Certificato SSL** e quindi scegliere **OK**.

			Site	Bindings	? X
Type http	Host Name	Port 80	IP Address	Binding Informa	Add Edit
			Add Site Bi	nding	? × emove
	pe: tps v ist name: Require Server Na	IP address All Unass me Indicatio	z igned m	V 443	
No No	L certificate: eb Cert issued by L it selected	AB-DC-RTP		V Select Vi	ew Close

• Ora si dispone di un nuovo binding SSL nel sito e tutto ciò che rimane è verificare che funzioni selezionando l'opzione **Sfoglia *:443 (https)** dal menu e assicurarsi che la pagina Web IIS predefinita utilizzi HTTPS:

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

Act	tions	
è.	Explore	
	Edit Permissions	
	Edit Site	
	Bindings	
Ē	Basic Settings	
	View Applications	
	View Virtual Directories	
Ma	nage Website	
2	Restart	
₽	Start	
	Stop	
	Browse Website	
0	Browse *:80 (http)	
0	Browse *:443 (https)	
	Advanced Settings	
	Configure	

• Ricordarsi di riavviare il servizio IIS dopo le modifiche alla configurazione. Utilizzare l'opzione **Restart** (Riavvia) nel riquadro Azioni.

Configurazione CUCM

 Accedere alla pagina Web di Servizi certificati Active Directory (<u>https://YOUR_SERVER_FQDN/certsrv/</u>) e scaricare il certificato CA

Microsoft Active Directory Certificate Services LAB-DC-RTP
Download a CA Certificate, Certificate Chain, or CRL
To trust certificates issued from this certification authority, install this CA certificate.
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.
CA certificate:
Encoding method:
DER O Base 64
Install CA certificate Download CA certificate Download CA certificate chain Download latest base CRL

• Passare a **Sicurezza** > **Gestione certificati** dalla pagina Amministrazione del sistema operativo e selezionare il pulsante **Carica catena certificati/certificati** per caricare il certificato CA con lo *scopo* impostato su *CAPF-trust*.

Upload Certificate/Certific	ate 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	

... A questo punto, è consigliabile caricare lo stesso certificato CA di *CallManager-trust* perché è necessario se la crittografia di segnalazione sicura è abilitata (o verrà abilitata) per gli endpoint, il che è probabile se il cluster è in modalità mista.

- Passare a Sistema > Parametri servizio. Selezionare il server Unified CM Publisher nel campo server e Cisco Certificate Authority Proxy Function nel campo Servizio.
- Impostare il valore di Autorità di certificazione su Endpoint nella CA in linea e immettere i valori nei campi Parametri CA in linea. Assicurarsi di utilizzare l'FQDN del server Web, il nome del modello di certificato creato in precedenza (CiscoRA), il tipo di CA come Microsoft CA e utilizzare le credenziali dell'account utente CiscoRA creato in precedenza

Service Par	rameter Configuration	
Save (Set to Default	
-Select Ser	ver and Service	
Server*	cucm125pubCUCM Voice/Video (Active)	$\overline{}$
Service*	Cisco Certificate Authority Proxy Function (Active)	
All paramet	ters apply only to the current server except parameters	that are in the cluster-wide group(s).
Cisco Certi	ificate Authority Proxy Function (Active) Paramet	ers on server cucm125pubCUCM Voice/Video (Activ Parameter Value
Certificate I	Issuer to Endpoint *	Online CA
Duration Of	Certificate Validity (in days) *	1825
Key Size *		1024
Maximum A	Ilowable Time For Key Generation *	30
Maximum Allowable Attempts for Key Generation *		3
-Online CA	A Parameters	
Online CA	Hostname	
		lab-dc-iis.michamen.com
Online CA	<u>\ Port</u>	443
Online CA	Template	CiscoRA
Online CA	Type_*	Microsoft CA
Online CA	Username	

• Una finestra pop indica che è necessario riavviare il servizio CAPF. Innanzitutto, attivare il servizio di registrazione certificati Cisco tramite Cisco Unified Serviceability > Strumenti > Attivazione servizio, selezionare l'entità di pubblicazione nel campo Server e selezionare la casella di controllo Servizio di registrazione certificati Cisco, quindi selezionare il pulsante Salva:

.......



Verifica

Verifica certificati IIS

Online CA Password

• Da un browser Web in un PC con connettività al server (preferibilmente nella stessa rete dell'editore CUCM) passare a URL:

https://YOUR_SERVER_FQDN/certsrv/

• Viene visualizzato l'avviso di certificato non attendibile. Aggiungere l'eccezione e controllare il certificato. Verificare che corrisponda all'FQDN previsto:



• Dopo aver accettato l'eccezione, è necessario eseguire l'autenticazione. A questo punto è necessario utilizzare in precedenza le credenziali configurate per l'account CiscoRA:

Authentication	n Required X		
?	https://lab-dc-iis.michamen.com is requesting your username and password.		
User Name:	ciscora		
Password:	••••••		
	OK Cancel		
	on conter		

• Dopo l'autenticazione è necessario essere in grado di visualizzare la pagina iniziale di Servizi certificati Active Directory:



Verifica configurazione CUCM

Eseguire la procedura normalmente descritta per installare un certificato LSC su uno dei telefoni.

Passaggio 1. Aprire la pagina Amministrazione di CallManager, Periferica e quindi Telefono

Passaggio 2. Selezionare il pulsante Trova per visualizzare i telefoni

Passaggio 3. Selezionare il telefono su cui installare LSC

Passaggio 4. Scorri verso il basso fino alle informazioni sulla funzione proxy dell'autorità di certificazione (CAPF)

Passaggio 5. Selezionare Installa/Aggiorna da Operazione certificato.

Passaggio 6. Selezionare la modalità di autenticazione. (By Null String è adatto ai fini del test)

Passaggio 7. Scorrere fino alla parte superiore della pagina e selezionare **save** (salva), quindi **Apply Config** (Applica configurazione) per il telefono.

Passaggio 8. Una volta riavviato il telefono e registrato di nuovo, usare il filtro Stato LSC per confermare che LSC è stato installato correttamente.

- Dal lato del server AD aprire MMC ed espandere lo snap-in Autorità di certificazione per selezionare la cartella Certificati rilasciati
- La voce relativa al telefono è visualizzata Nella visualizzazione di riepilogo, sono riportati alcuni dettagli:
 - ID richiesta: numero di sequenza univoco
 - Nome richiedente: è necessario visualizzare il nome utente dell'account CiscoRA configurato
 - · Modello di certificato: è necessario visualizzare il nome del modello CiscoRA creato
 - Issued Common Name: è necessario visualizzare il modello del telefono aggiunto dal nome del dispositivo
 - Data di validità e data di scadenza del certificato



Collegamenti correlati

- <u>Risoluzione dei problemi relativi a CAPF Online CA</u>
- Documentazione e supporto tecnico Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).