Configurare RADIUS per Windows 2008 Server dei criteri di rete - WAAS AAA

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Procedura di configurazione
1. Gestore centrale WAAS
2. Windows 2008 R2 - Configurazione Server dei criteri di rete
3. Configurazione WAAS CM per account utente RADIUS
Verifica
Risoluzione dei problemi
Informazioni correlate

Introduzione

In questo documento viene descritta la procedura di configurazione di RADIUS (Remote Authentication Dial-In User Service) in Cisco Wide Area Application Services (WAAS) e Windows 2008 R2 Network Policy Server (NPS).

La configurazione WAAS predefinita utilizza l'autenticazione locale. Cisco WAAS supporta RADIUS e Terminal Access Controller Access-Control System (TACACS+) anche per l'autenticazione, l'autorizzazione e l'accounting (AAA). Questo documento descrive la configurazione per un solo dispositivo. Tuttavia, è possibile eseguire questa operazione anche nel gruppo di dispositivi. Tutta la configurazione deve essere applicata tramite l'interfaccia grafica di WAAS CM.

La configurazione generale di WAAS AAA è disponibile nella <u>Cisco Wide Area Application</u> <u>Services Configuration Guide</u> nel capitolo Configuring Administrative Login Authentication, Authorization, and Accounting.

Contributo di Hamilan Gnanabaskaran, Cisco TAC Engineer.

Modificato da Sanaz Tayyar, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- WAAS 5.x o 6.x
- Server dei criteri di rete Windows
- AAA RADIUS

Componenti usati

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

- Cisco WAAS Virtual Central Manager (vCM)
- WAAS 6.2.3.b
- Windows 2008 NPS

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.

Prodotti correlati

Il documento può essere applicato anche alle seguenti versioni hardware e software:

- vWAAS, ISR-WAAS e tutti gli accessori WAAS
- WAAS 5.x o WAAS 6.x
- WAAS come Central Manager, Application Accelerator

Nota: APPNAV-XE non supporta questa configurazione. Il router AAA invia la configurazione ad APPNAV-XE.

Procedura di configurazione

È necessario applicare le seguenti configurazioni:

- 1. Gestore centrale WAAS
 - 1.1 Configurazione AAA RADIUS
 - 1.2 Configurazione dell'autenticazione AAA
- 2. Windows 2008 R2 Configurazione Server dei criteri di rete
 - 2.1 Configurazione dei client RADIUS
 - 2.2 Configurazione dei criteri di rete
- 3. Configurazione WAAS CM per account utente RADIUS
- 1. Gestore centrale WAAS
- 1.1 In WAAS Central Manager crea il server RADIUS in

Configurazione>Sicurezza>AAA>RADIUS.

Cisco Wide Area Applica Devices > vCM-POD4-Primary > Configure > Sec RADIUS Server Settings for Cent	tion Services urity > AAA > RADIUS ral Manager, vCM-POD	Home Device Groups VCM-POD4-Primary 4-Primary Print	Devices AppNav Clusters Loc Configure Monitor Apply Defaults Remove Se	ations Admin I ▼ ttings	avalon Logout Help About		
		RADIUS	Server Settings				
Time to Wait.*	5 (s	econds) (1-20)					
Number of Retransmits:*	2 🗘						
Shared Encryption Key:							
Server 1 Name:	10.66.86.125		Server 1 Port:	1645			
Server 2 Name:			Server 2 Port:				
Server 3 Name:			Server 3 Port:				
Server 4 Name:			Server 4 Port:				
Server 5 Name:			Server 5 Port:				
To use RADIUS for Login or Configuration Authentication, please go to the Authentication Methods page.							
Note: * - Required Field							

1.2 Configurare il metodo di autenticazione in modo che rifletta RADIUS in Configurazione>Protezione>AAA>Metodi di autenticazione.

Il metodo di autenticazione primaria viene scelto come RADIUS, mentre il metodo di autenticazione secondaria viene scelto come locale. Pertanto, in caso di guasto di RADIUS, il cliente può accedere tramite l'account locale.

CISCO Cisco Wide Area Application Services Devices > CM-Secondary-WAVE594 > Configure > Security > AAA > Authenti	Home Device Groups Devices AppNav Clusters Locations CM-Secondary-WAVE594 Configure Monitor Admin cation Methods
Authentication and Authorization Methods for Cent	ral Manager, CM-Seco 🥝 Print 🔎 Apply Defaults 👔 Remove Settings
	Authentication and Authorization Methods
Failover to next available authentication method:	0
Use only local admin account to enable privilege exec level:	
Authentication Login Methods:	i It is highly recommended to set the authentication and authorization methods in the su
Primary Login Method:*	RADIUS
Secondary Login Method:	local 📀
Tertiary Login Method:	Do Not Set
Quaternary Login Method:	Do Not Set 😒
Authorization Methods:	 Ø
Primary Configuration Method:*	RADIUS
Secondary Configuration Method:	local
Tertiary Configuration Method:	Do Not Set
Quaternary Configuration Method:	Do Not Set
	Windows Authentication
Refresh Authentication Status	Show Windows Authentication Status
Note: * - Required Field	

2. Windows 2008 R2 - Configurazione Server dei criteri di rete

2.1 Nel server Windows 2008 R2 - Server dei criteri di rete, creare l'indirizzo IP del dispositivo WAAS come client RADIUS.

RADIUS Clients Remote RADIUS Server G Policies Network Access Protection Accounting	RADIUS clients allow you to specify the network access servers, that provide access to your network. Friendly Name IP Address Device Manufacturer NAP-Capable Status vCM 10.66.86.121 RADIUS Standard No Enabled
Templates Management	VCM Properties X Settings Advanced X Enable this RADIUS client Setect an existing template: X Name and Address Friendy name: X VCM Address (IP or DNS): X 10.66.86.121 Verfy Verfy Shared Secret Select an existing Shared Secrets template: X None X X To manually type a shared secret, click Manual. To automatically generate a shared secret entered here. Shared secrets are case-sensitive. X To manually type a shared secret are essensitive. X X Manual C Generate Confirm shared secret: X OK Cancel Apply

2.2 Nel server Windows 2008 R2 - Server dei criteri di rete creare un criterio di rete che corrisponda ai dispositivi WAAS e consenta l'autenticazione.



In LAB questi parametri devono essere selezionati in Server dei criteri di rete >Criteri>Criteri di rete.

review Conditions Constraints Settings Policy name: IDECY WAAS Policy State If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. If enabled Policy enabled Access Permission If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. (What is access permission?) If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. (What is access permission?) If grant access. Grant access if the connection request matches this policy. If policy enabled If one quest matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user account is. If the connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or very expectic, but netther is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Image: The prove of network access server: Image: The prove of network access server: Image: The perfied If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Image: The perine difference	ICY_WAAS Pro	perties											
Policy name: POLICY_WAAS Policy name: POLICY_WAAS Policy State If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. Policy enabled Access Permission f conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission? G Grant access. Grant access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access a the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only: do not evaluate the dial in properties of user accounts . Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific. Dual there is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server: Densection performed to the intervent of the intervent access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server: Densection the network access server: Densection termetation termetation termetation termetation termetation termet	verview Condition	ns Constraints	s Settings										
Policy State If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. ✓ Policy enabled Access Permission If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. <u>What is access permission?</u> • Grant access. Grant access if the connection request matches this policy. • Deny access. Deny access if the connection request matches this policy. Ignore user account dial-in properties. If the connection request matches the conditions and constraints of this network policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts. Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but nether is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. • Vendor specific: Image:	olicy name:	POLI	CY_WAAS										
Policy State If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. If Policy enabled Access Permission If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission? If a Grant access Grant access if the connection request matches this policy. Image: Deny access. Deny access if the connection request matches this policy. Image: Deny access. Deny access if the connection request matches this policy. Image: Image: Deny access if the connection request matches this policy. Image: Image: Deny access if the connection request matches this policy. Image: Image: Deny access if the connection request matches this policy. Image: Image: Deny access if the connection request matches this policy. Image: Image: Deny access if the connection request matches this policy. Image: Image: Deny access image: Deny access image: Deny access provement and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts . Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access point, select Unspecified. Image: Type of network access server: Unspecified Image: Deny dense pecific: <													
 ✓ Policy enabled Access Permission If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission? Grant access. Grant access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Ignore user account dial-in properties. If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only: do not evaluate the dial-in properties of user accounts. Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access point, select Unspecified. Type of network access server: Unspecified Unspecified Vendor specific: 10 20 0K Cancel Access Access 0K Cancel Access Access	Policy State	evaluates this p	olicy while p	performing	; authorizati	on. If disable	d, NPS doe	es not e	valuate this po	licy.			
Access Permission If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission? Grant access. Grant access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Ignore user account dial-in properties. If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts. Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access point, select Unspecified. Type of network access server: Unspecified Vendor specific: 10 OK Cancel Access Cancel	Policy enabl	ed											
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. <u>What is access permission?</u> If access. Grant access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Ignore user account dial-in properties. If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts. Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access point, select Unspecified. If type of network access server: Unspecified Vendor specific: 10 20 0K Cancel	Access Permiss	on											
 Grant access. Grant access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Ignore user account dial-in properties. If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts. Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specifie, but nether is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server: Unspecified Vendor specific: 10 	If conditions ar access. <u>What i</u>	d constraints of access permi	the networ ssion?	rk policy i	match the o	connection r	equest, the	policy	can either gra	ant acc	cess or d	eny	
 Deny access. Deny access if the connection request matches this policy. Ignore user account dial-in properties. If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts . Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server: Unspecified Vendor specific: 10 20K Cancel 	 Grant access 	. Grant access i	f the conne	ection requ	Jest matche	s this policy.							
I Ignore user account dial-in properties. If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts . Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server: Unspecified Vendor specific: 10 20 C Cancel C Andit	O Deny access	Deny access if	the connec	ction requ	est matche	s this policy.							
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts . Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server: Unspecified Vendor specific: 10 0K Cancel Andite	🗌 Ignore user a	count dial-in pr	operties.										
Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Image: Type of network access server: Image: Unspecified Image: Vendor specific: Image: Unspecified Image: Unspecif	If the connect authorization	on request mate vith network pol	ches the cor icy only; do	nditions a not evalu	nd constraii iate the dial	nts of this ne in properties	twork policy of user acc	and th	e policy grants	acce	ss, perfor	m	
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server: Unspecified Vendor specific: 10 CMC Cancel Ander	-Network conne	tion method -											
	Select the type or Vendor specifi select Unspecifi	f network acce c, but neither is ed.	ss server tha required. If	at sends t f your net	the connect work acces	tion request t s server is ar	o NPS. You 1 802.1X au	u can se thentic	elect either the ating switch or	netwo wirele	ork acces ess accese	s serve s point,	er type '
Unspecified Vendor specific: 10 CMC Cancel Apple	• Type of net	ork access sen	/er:										
C Vendor specific:	Unspecified				_]							
	C Vendor spec	ific:											
OK Cancel Apple	10												
									OK	1	Cancel	1	Annlu

La condizione può essere associata al nome descrittivo del client Radius. È possibile utilizzare altri metodi, ad esempio indirizzo IP.

POLICY_WAAS Properties		×
Overview Conditions Constra	raints Settings	
Configure the conditions for this	is network policy	
If conditions match the connect connection request, NPS skips	ction request, NPS uses this policy to authorize the connection request. If conditions do not match the is this policy and evaluates other policies, if additional policies are configured.	
Condition	Value	
Ulent Friendly Name		
windows Groups	ANJU WAAJ	
1		
Condition description:		
The Windows Groups condition	on specifies that the connecting user or computer must belong to one of the selected groups.	
	Add Edit Remov	/e
	OK Cancel	Ápplu
		אואאב

Metodi di autenticazione come autenticazione non crittografata (PAP, SPAP).

Overview Conditions Constraints Settings Configure the constraints for this network policy. If all constraints are not matched by the connection request, network access is denied. Constraints: Constraints
Configure the constraints for this network policy. If all constraints are not matched by the connection request, network access is denied. Constraints:
Constraints Authentication Methods Authentication Methods Allow access only to those clients that authenticate with the specified methods. Image: Authentication Methods EAP types are negotiated between NPS and the client in the order in which they are listed. Image: Called Station ID EAP Types: Image: Day and time restrictions Move Up Image: NAS Port Type Move Down Add Edt
Less secure authentication methods: Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired Encrypted authentication (CHAP) V Unencrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method Perform machine health check only

Service-Type impostato su Administrative.

POLICY_WAAS Properties				×
Overview Conditions Constraints Setting				
Overview Conditions Constraints Settings Configure the settings for this network policy. If conditions and constraints match the constraints match the constraints Settings: RADIUS Attributes Settings: Standard Image: Vendor Specific Network Access Protection NAP Enforcement Image: Extended State Routing and Remote Access Multilink and Bandwidth Allocation Protocol (BAP) IP Filters	To send additional attribut then click Edit. If you do r your RADIUS client docur Attributes: Name Value Service-Type Admi	e grants access, settings ar res to RADIUS clients, sele not configure an attribute, i mentation for required attrib	re applied. ect a RADIUS standard attribut t is not sent to RADIUS client butes.	.te, and s. See
Encryption	Add Ed	it Remove	OK Cancel	Ându
			UK Cancel	

Attributo specifico del fornitore come Cisco-AV-Pair (Shell:priv-lvl=15).

POLICY_WAAS Properties		X						
Overview Conditions Constraints Settings	s							
Configure the settings for this network policy. If conditions and constraints match the connection request and the policy grants access, settings are applied. Settings:								
RADIUS Attributes	To send additional attributes to RADIUS clients, sei then click Edit. If you do not configure an attribute, your RADIUS client documentation for required attri	lect a Vendor Specific attribute, and it is not sent to RADIUS clients. See ibutes.						
NAP Enforcement	Attributes:							
🕎 Extended State	Name Vendor Value							
Routing and Remote Access	Cisco-AV-Pair Cisco shell:priv-lvl=15							
Multilink and Bandwidth Allocation Protocol (BAP) IP Filters Encryption								
	Add Edit Remove							
	[OK Cancel Apply						

Consenti Accesso Completo Alla Rete.

POLICY_WAAS Properties	2
Overview Conditions Constraints Settings	
Overview Conditions Constraints Settings Configure the settings for this network policy. If conditions and constraints match the connection request and the policy grants access, settings are Settings: RADIUS Attributes Specify whether you want to enforce Network Access Standard Vendor Specific Specify whether you want to enforce Network Access Network Access Protection Allow full network access for clients whe the policy. Use this option for reporting mode. NAP Enforcement Allow full network access for a limited time Allows unrestricted network access on the restricted network. Multilink and Bandwidth Allocation Protocol (BAP) Multilink and Bandwidth Allocation Protocol (BAP) IP Filters Allow limited access Non-compliant clients are allowed access only to a Remediation Server Group, a Trouble Configure.	eshooting URL, or both, click
Auto remediation Auto remediation of client computers Automatically remediate computers that do not r in this policy.	neet health requirements defined
Automatically remediate computers that do not r in this policy.	Neet health requirements defined

3. Configurazione WAAS CM per account utente RADIUS

Configurare un utente in RADIUS con il livello di privilegio 15 o 1, non consente l'accesso all'interfaccia utente di WAAS CM. Il database CMS gestisce un elenco di utenti, ruoli e domini separati dal server AAA esterno.

Dopo aver configurato correttamente il server AAA esterno per l'autenticazione di un utente, è necessario configurare l'interfaccia utente grafica di CM in modo da assegnare all'utente i ruoli e i domini necessari per il funzionamento nell'interfaccia utente di CM.

Se l'utente RADIUS non si trova nella CM sotto l'utente, quando si accede alla GUI con tale utente, l'account dell'utente non dispone dei privilegi necessari per accedere a nessuna delle pagine di Gestione centrale. Rivolgersi all'amministratore per informazioni sui ruoli e i domini di cui è stato eseguito il provisioning. Questo massaggio viene visualizzato.



Configurazione del nome utente locale in WAAS CM senza password.

ahaha		Home Device Groups	Devices AppNav Clusters	Locations	avalon Logout Help About				
cisco Cisco Wide Are	ea Application Services	Dashboard Configure	Monitor Admir	n 🔻					
Home > Admin > AAA > Users	ome > Admin > AAA > Users								
Account Management Role Ma	nagement Domain Management								
Modifying User Account	Modifying User Account, avalon 👔 Delete 🤤 Print								
		Account	Information						
Usemame:*	avalon								
WAE Device Manager User:			Device Manager Access:	Read Only 0					
Local User:			CLI Privilege Level:	0 (normal user)					
Password:									
Confirm Password:									
		User In	formation						
First Name:			Last Name:						
Phone Number:			Email Address:						
Job Title:			Department:						
	Roles Domains								
60 admin	A admin There are no Domains assigned.								
Failed Creation on Devices Locked-out of Devices									
This user exists on all devices.			This user is not locked out of	of any device.					
Comments									

Il nome utente deve essere associato ai ruoli corretti in Gestione ruoli per ogni utente.

$\bullet \bullet \bullet \checkmark >$		⊜ 10.66.86.121	Ċ
ahaha cisco Cisco (Nide Area Application Services	Home Device Groups Devices App Dashboard Configure V Monitor	Nav Clusters Locations
Home > Admin > AAA >	Users		
Account Management	Role Management Domain Manageme	nt	
Refresh Table	📑 Assign all Roles 🛛 😰 Remove all I	Roles	
Roles			Ite
Filter: Name	C Match if: contains	Go Clear Filt	ter
	Role		Comments
🗶 60 L2			
I Galanin		Admin role	

Se l'utente deve disporre di accesso in sola lettura o di accesso limitato, è possibile configurarlo in ruoli.

	€ 10.66.86.121
CISCO Cisco Wide Area Application Services	Home Device Groups Devices AppNav Clusters Locations Dashboard Configure Monitor Admin
Home > Admin > AAA > Roles Modifying Role, L2 In Delete Print	
	Role Definition
Name:* L2	
Enabled Services:	
	Comments

Verifica

Nei dispositivi WAAS viene eseguito il push di questa configurazione.

```
chiave radius-server ****
host radius-server 10.66.86.125 auth-port 1645
!
```

```
autenticazione accesso locale abilitazione secondario
```

raggio di accesso autenticazione abilitazione primario configurazione di autenticazione locale abilitazione secondaria raggio di configurazione autenticazione abilitazione primario autenticazione failover server non raggiungibile

<u>Cisco CLI Analyzer (solo utenti registrati) supporta alcuni comandi</u> show. Usare Cisco CLI Analyzer per visualizzare un'analisi dell'output del comando show.

• autenticazione - Configura autenticazione

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

- Controllare i registri di dominio di Windows
- #debug aaa authorization da WAAS CM CLI

Informazioni correlate

- Configurazione delle impostazioni di autenticazione del server RADIUS su WAAS
- Applicazione di Server dei criteri di rete a Windows Server 2008

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).