Configurazione di un Syslog Server esterno su ISE

Sommario

Introduzione
<u>Prerequisiti</u>
Requisiti
Componenti usati
Premesse
Configurazione
Configurazione destinazione registrazione remota (UDP Syslog)
Esempio
Configurazione destinazione remota in Categorie di registrazione
Informazioni sulle categorie
<u>Verifica e risoluzione dei problemi</u>

Introduzione

Questo documento descrive come configurare External Syslog Server su ISE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Services Engine (ISE).
- Server Syslog

Componenti usati

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

- Identity Services Engine (ISE) versione 3.3.
- Kiwi Syslog Server v1.2.1.4

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

I messaggi syslog provenienti da ISE vengono raccolti e archiviati da log collector. Questi agenti di raccolta log vengono assegnati ai nodi di monitoraggio in modo che MnT memorizzi i log raccolti localmente.

Per raccogliere i registri esternamente, è necessario configurare i server syslog esterni, denominati destinazioni. I log vengono classificati in varie categorie predefinite.

È possibile personalizzare l'output di registrazione modificando le categorie in base alle destinazioni, al livello di gravità e così via.

Configurazione

È possibile utilizzare l'interfaccia Web per creare destinazioni remote del server syslog a cui vengono inviati i messaggi del registro eventi di sistema. I messaggi di log vengono inviati alle destinazioni remote del server syslog in base allo standard del protocollo syslog (vedere RFC-3164).

Configurazione destinazione registrazione remota (UDP Syslog)



Nell'interfaccia utente di Cisco ISE, fare clic sull'icona del menu (

) e scegliere Amministrazione>Sistema>Log>Destinazioni di log remoto > Fare clic su Aggiungi.



Nota: questo esempio di configurazione si basa su uno screenshot intitolato: Configurazione destinazione di registrazione remota.

- Nome come Remote_Kiwi_Syslog, qui è possibile immettere il nome del server Syslog remoto, utilizzato per scopi descrittivi.
- Tipo di destinazione come UDP Syslog, in questo esempio di configurazione viene utilizzato UDP Syslog; tuttavia, è possibile configurare altre opzioni dall'elenco a discesa Tipo di destinazione:

UDP Syslog: utilizzato per l'invio di messaggi syslog su UDP, adatto per la registrazione rapida e leggera.

TCP Syslog: utilizzato per l'invio di messaggi syslog tramite TCP, che fornisce affidabilità con controllo degli errori e funzionalità di ritrasmissione.

Secure Syslog: si riferisce ai messaggi syslog inviati tramite TCP con crittografia TLS, che garantiscono l'integrità e la riservatezza dei dati.

- Status as Enabled, è necessario scegliere Enabled dall'elenco a discesa Status.
- Descrizione, facoltativamente è possibile inserire una breve descrizione della nuova destinazione.
- Indirizzo host/IP, in cui è possibile immettere l'indirizzo IP o il nome host del server di destinazione in cui sono archiviati i registri. Cisco ISE supporta i formati IPv4 e IPv6 per la registrazione.



Nota: se si intende configurare un server syslog con FQDN, è necessario configurare la memorizzazione nella cache DNS per evitare l'impatto sulle prestazioni. Senza la cache DNS, ISE esegue query sul server DNS ogni volta che un pacchetto syslog deve essere inviato alla destinazione di registrazione remota configurata con FQDN. Questo ha un forte impatto sulle prestazioni di ISE.

Utilizzare service cache enableil comando in tutti i PSN della distribuzione per risolvere il problema:

Esempio

ise/admin(config)# service cache enable hosts ttl 180

• **Port** as **514**, in questo esempio di configurazione, il server Syslog Kiwi è in ascolto sulla porta **514**, che è la porta predefinita per i messaggi syslog UDP. Tuttavia, gli utenti possono modificare questo numero di porta in qualsiasi valore compreso tra 1 e 65535. Assicurarsi che la porta desiderata non sia bloccata da alcun firewall.

• Codice struttura come LOCAL6, è possibile scegliere il codice struttura syslog da utilizzare per la registrazione dall'elenco a discesa. Le opzioni valide sono da Local0 a Local7.

• Lunghezza massima: 1024, in cui è possibile immettere la lunghezza massima dei messaggi di destinazione del log remoto. La lunghezza massima è impostata su 1024 per default nella versione ISE 3.3. I valori sono compresi tra 200 e 1024 byte.



Nota: per evitare di inviare messaggi troncati alla destinazione di registrazione remota, è possibile modificare la lunghezza massima come 8192.

• Includi allarmi per questa destinazione, per semplificarne la gestione, in questo esempio di configurazione l'opzione Includi allarmi per questa destinazione non è selezionata; tuttavia, quando si seleziona questa casella di controllo, vengono inviati messaggi di allarme anche al server remoto.

• L'opzione Conformità alla RFC 3164 è selezionata. Quando si seleziona questa casella di controllo, i delimitatori (, ; { } \\\) nei messaggi syslog inviati ai server remoti non vengono ignorati anche se si utilizza la barra rovesciata (\).

Al termine della configurazione, fare clic su Save (Salva).

Dopo il salvataggio, il sistema visualizzerà questo avviso: si è scelto di creare una connessione non protetta (TCP/UDP) al server. Continuare?, fare clic su Sì.

	dentity Services	Engine			Administration / System								Q	۵	?	Q
PI	Bookmarks	Deployment	Licensing	Certific	cates	Logging	Maintenance	Upgrade	Health Check	s Backup & Restore	Admin Access	Settings				
5	Dashboard	Log Settings			emote Logai	ng Targets List	> Remote Kiwi Svslog									
I ^{ld}	Context Visibility	Remote Logging	Targets		ogging T	arget										
*	Operations	Message Catalog	a a a a a a a a a a a a a a a a a a a													
U	Policy	Collection Filters			* Name		Remote_Ki	wi_Syslog	Target Type	UDP SysLog						
2	Administration				Description		Remote Log	ging Target	Status	Enabled V						
កា	Work Centers				* Host / IP	Address	10.:									
					* Port		514		(Valid Range	1 to 65535)						
?	Interactive Help				Facility Co	de	LOCAL6									
					* Maximun	n Length	1024		(Valid Range	200 to 8192)						
					Include Ala	arms For this	Target									
					Comply to	RFC 3164	0									
													Save		R	eset

Configurazione destinazione remota

•

Configurazione destinazione remota in Categorie di registrazione

Cisco ISE invia eventi verificabili alla destinazione syslog. Una volta configurata la destinazione di registrazione remota, è necessario mappare la **destinazione di registrazione remota** alle categorie previste per inoltrare gli eventi controllabili.

Le destinazioni di registrazione possono quindi essere mappate a ognuna di queste categorie di registrazione. I registri eventi generati da queste categorie di registro vengono generati solo dai nodi PSN e possono essere configurati in modo da inviare i registri rilevanti al server Syslog remoto a seconda dei servizi abilitati in tali nodi:

Audit AAA

•

•

•

•

Diagnostica AAA

Contabilità

MDM esterno

•

ID passivo

•

Controllo della postura e del provisioning client

Diagnostica provisioning postura e client

Profiler

٠

•

•

•

•

I registri eventi generati da queste categorie di registro vengono generati da tutti i nodi nella distribuzione e possono essere configurati in modo da inviare i registri pertinenti al server Syslog remoto:

Audit amministrativo e operativo

Diagnostica di sistema

Statistiche di sistema

In questo esempio di configurazione, si configurerà la destinazione remota in quattro categorie di registrazione, queste 3 per inviare i log del traffico di autenticazione: **Autenticazioni passate**, **Tentativi non riusciti** e **Accounting Radius** e questa categoria per il traffico di registrazione dell'amministratore ISE:



Nota: questo esempio di configurazione si basa su uno screenshot intitolato: Configurazione destinazione di registrazione remota

Nell'interfaccia utente di Cisco ISE, fare clic sull'icona Menu (



), quindi selezionare Amministrazione>Sistema>Registrazione>Categorie di registrazione e fare clic sulla categoria richiesta (Autenticazioni passate, Tentativi non riusciti e Accounting Radius).

Passaggio 1-Livello di gravità del registro: un messaggio di evento è associato a un livello di gravità, che consente a un amministratore di filtrare i messaggi e di assegnare loro la priorità. Selezionare il livello di gravità del registro, se necessario. Per alcune categorie di registrazione, questo valore è impostato per impostazione predefinita e non è possibile modificarlo. Per alcune categorie di registrazione, è possibile scegliere uno dei seguenti livelli di gravità da un elenco a discesa:

FATALE: livello di emergenza. Questo livello significa che non è possibile utilizzare Cisco ISE e che è necessario eseguire immediatamente l'azione necessaria.

ERRORE: questo livello indica una condizione di errore critica.

•

AVVERTENZA: questo livello indica una condizione normale ma significativa. Questo è il livello predefinito impostato per molte categorie di registrazione.

INFORMAZIONI: questo livello indica un messaggio informativo.

•

DEBUG: questo livello indica un messaggio di bug diagnostico.

Passaggio 2- Log locale: questa casella di controllo abilita la generazione del log locale. Ciò significa che i registri generati dai nomi PSN vengono salvati anche nel nome PSN specifico che genera il registro. È consigliabile mantenere la configurazione predefinita

Passo 3 - Targets: quest'area consente di scegliere le destinazioni per una categoria di logging trasferendo le destinazioni tra l'area Available e l'area Selected utilizzando le icone a freccia sinistra e destra.

L'area Available contiene le destinazioni di registrazione esistenti, sia locali (predefinite) che esterne (definite dall'utente).

L'area Selezionati, inizialmente vuota, consente di visualizzare gli oggetti scelti per la categoria.

Passaggio 4- Ripetere dal passaggio 1 al passaggio 3 per aggiungere Destinazione remota nelle categorie Tentativi non riusciti e Accounting Radius.

	dentity Services	Engine				Adm	inistration /	System				Q (
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings	
	Dashboard	Log Settings	Targets			Passed Authentications						
- N	Context Visibility	Logging Categor	ies	Logging C	Category							
×	Operations	Message Catalog	9	Name	P	assed Authentications						
Ð	Policy	Collection Filters		Log Severi	ty Level I	INFO						
20	Administration					Log level can not be cha	inged.)					
តា	Work Centers			Local Logg	jing							
				Targets	A	vailable:	Selec	ted:				
	Interactive Help							ogCollector				
								emote_Kiwi_Syslog				
												Save

Mapping delle destinazioni remote alle categorie previste

Passaggio 5- Verificare che la destinazione remota sia inclusa nelle categorie richieste.È necessario essere in grado di visualizzare la destinazione remota appena aggiunta.

In questa schermata è possibile visualizzare la destinazione remota Remote_Kiwi_Syslog mappata alle categorie richieste.

	dentity Services E	Engine									(Administration / S	System	
Щ	Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup &	Restore	Admin Access	Settings		
	Dashboard	Log Settings												
	Context Visibility	Remote Logging	Targets	Logo	Logging Categories									
a./	Operations	Logging Categor	ies											
	operationa	Message Catalog	3											
<u> </u>	Policy				Parent Categor	ny	Ca	itegory	Tar	gets			Severity	Local Log
	Administration				AAA Audit				Lo	aCollector			INFO	enable
	Work Centers			6					Lo	gCollector,Pro	filerRadiusProbe,Rem	note_Kiwi_Syslog	INFO	enable
									Lo	gCollector,Pro	filerRadiusProbe,Rem	note_Kiwi_Syslog	INFO	enable
	Interactive Help				AAA Diagnosti	cs			Lo	aCollector			WARN	enable
													WARN	enable
													WARN	enable
								entity Stores Diagnostics					WARN	enable
													WARN	enable
									Lo	gCollector			WARN	enable
									Lo	gCollector			INFO	enable
									Lo	gCollector			INFO	enable
				0					Lo	gCollector			INFO	enable
				0					Lo	gCollector			WARN	enable
				0	ACI Binding				Lo	gCollector			INFO	enable
				0	Accounting				Lo	gCollector			INFO	enable
				$\overline{(}$					Lo	gCollector,Pro	filerRadiusProbe,Rem	note_Kiwi_Syslog	INFO	enable
				0					Log	gCollector			INFO	enable
				0	Administrative	and Operational Audit			Audit Log	gCollector,Ren	note_Kiwi_Syslog		INFO	enable
				0	External MDM				Lo	gCollector			INFO	enable
				0	PassiveID				Lo	gCollector			INFO	enable
				0	Posture and Cli	ient Provisioning Audit			Audit Pro	ofilerRadiusPro	obe,LogCollector		INFO	enable
				0	Posture and Cli	ient Provisioning Diagn	ostics Po		Diagno Lo	gCollector			WARN	enable
				0	Profiler				Lo	gCollector			INFO	enable
				0	System Diagno	stics			Lo	gCollector			WARN	enable
				0									WARN	enable
				0									WARN	enable
				0					Lo	gCollector			INFO	enable
				0					Lo	gCollector			INFO	enable
				0	System Statisti	ics			Lo	gCollector			INFO	enable

Verifica delle categorie

Informazioni sulle categorie

Quando si verifica un evento, viene generato un messaggio. Esistono diversi tipi di messaggi di eventi generati da più strutture, quali il kernel, la posta, il livello utente e così via.

Questi errori vengono classificati all'interno del Catalogo messaggi e questi eventi sono organizzati gerarchicamente in categorie.

Queste categorie dispongono di Categorie padre contenenti una o alcune categorie.

Categoria padre	Categoria
Audit AAA	Audit AAA Tentativi non riusciti Autenticazione superata
Diagnostica AAA	Diagnostica AAA Autenticazione e autorizzazione

	dell'amministratore Diagnostica flusso di autenticazione Diagnostica archivio identità Diagnostica criteri
	Guest
Contabilità	Contabilità Accounting Radius
Audit amministrativo e operativo	Audit amministrativo e operativo
Controllo della postura e del provisioning client	Controllo della postura e del provisioning client
Diagnostica provisioning postura e client	Diagnostica provisioning postura e client
Profiler	Profiler
Diagnostica di sistema	Diagnostica di sistema Gestione distribuita Diagnostica delle operazioni interne
Statistiche di sistema	Statistiche di sistema

In questa schermata è possibile vedere che **Guest** è una classe messaggio e classificato come **categoria Guest**. Questa categoria Guest ha una categoria padre chiamata **AAA Diagnostics**.

\equiv $\frac{1}{1000}$ Identity Service	s Engine									Administration / System		
JI Bookmarks	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings		
Dashboard	Log Settings Remote Logging T Logging Categorie	argets IS	Mess	age Ca	italog							
Operations Policy	Collection Filters											
Administration			Category	Name			Message Class	Message Code	Message Text		Message Description	Severity
Work Centers			guest				K	96001	Cuest user be	e estered the quest portal losis page		INFO
			Guest				Guest	86002	Sponso Guest	t user has entered the quest portal login page	Sponsor has suspended a guest user account	INFO
② Interactive Help			Guest				Guest	86003	Sponsor has e	mabled a guest user account	Sponsor has enabled a guest user account	INFO
			Guest				Guest	86004	Guest user ha	s changed the password	Guest user has changed the password	INFO
			Guest				Guest	86005	Guest user ha	s accepted the Use Policy	Guest user has accepted the use policy	INFO
			Guest				Guest	86006	Guest user ac	count is created	Guest user account is created	INFO
			Guest				Guest	86007	Guest user ac	count is updated	Guest user account is updated	INFO
			Guest				Guest	86008	Guest user ac	count is deleted	Guest user account is deleted	INFO
			Guest				Guest	86009	Guest user is	not found	Guest user record is not found in the database	INFO
			Guest				Guest	86010	Guest user au	thentication failed	Guest user authentication failed. Please check your password and account permis	INFO
			Guest				Guest	86011	Guest user is	not enabled	Guest user authentication failed. User is not enabled. Please contact your system	INFO
			Guest				Guest	86012	User declined	Access-Use Policy	Guest User must accept Access-Use policy before network access is granted	INFO
			Guest				Guest	86013	Portal not four	nd	Portal is not found in the database. Please contact your system administrator	INFO
			Guest				Guest	86014	User is susper	nded	User authentication failed. User account is suspended	INFO
			Guest				Guest	86015	Invalid Passwo	ord Change	Invalid password change. Use correct password based on the password policy	INFO
			0				0	05016			The sector from a sector back sector of the thread of the	INITO .

Catalogo messaggi

Verifica e risoluzione dei problemi

Effettuare un dump TCP sulla destinazione di registrazione remota è il passaggio più rapido per la risoluzione dei problemi e la verifica per confermare se gli eventi di registrazione vengono inviati o meno.

È necessario eseguire l'acquisizione dal PSN che autentica l'utente perché il PSN genererà messaggi di log e questi messaggi verranno inviati alla destinazione remota



Nell'interfaccia utente di Cisco ISE, fare clic sull'icona del menu (

), quindi selezionare **Operations**> **Troubleshoot**>**TCP Dump**> Fare clic su **Add**.

• È necessario filtrare il traffico, aggiungere il campo filtro ip host <indirizzo_IP_destinazione_remota>.

• È necessario acquisire da PSN che gestisce le autenticazioni.

$\equiv \frac{\mathrm{alloch}}{\mathrm{cisco}}$ Identity Services	Engine	Operations / Troubleshoot
Bookmarks	Diagnostic Tools Download L	Logs Debug Wizard
Dashboard	General Tools ~	TGP Durse > New
Context Visibility	RADIUS Authentication Troubl Execute Network Device Com	Add TCP Dump
Policy	Evaluate Configuration Validat Posture Troubleshooting	Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.
2. Administration	Agentiess Posture Troublesho	SSPT33A V
Work Centers	EndPoint Debug TCP Dump Session Trace Tests	Network Interface" Glabblitthemet 0 [Up, Running] V ()
Interactive Help	TrustSec Tools	
		Filter for the set of
		Eq: ip host 10.77.122.123 and not 10.177.122.119
		File Name Remote Syslog Server Test
		Aspository 🗸 🕐
		File Size
		Mo Mo
		Limit to T File(a)
		Time Limit 0
		Minule(s) Promiscuoud Mode
		Cancel Save Save and Run

Dump TCP

In questa schermata, puoi vedere come ISE sta inviando messaggi Syslog per il traffico di registrazione dell'amministratore ISE.

							SSPT33A_GigabitEthernet 5.pcap	
	a 🔊	늘 📾 🔯 I	a o 👝 🚽	s 💩 🛣 🕹 🔳 🛯	• •	a e 🚥		
Apply :	a display filter		10	10	6	11		
NO.	1 2024-07-2	5 10.20.27 235//1	Source	Destination	Svelog	Length	INTO LOCALE NOTICE: 11: 25 11:20:37 CODT334 CTSE Administrative and Operational Audit ###############################	-05.00 0000012801
	2 2024-07-2	5 10:29:49.056594	10.201.231.67	10.201.231.90	Systog	423	Inclais NorTrE- Jul 25 11:23:49 (SPT336 CTE_Administrative_and_Operational_Audit 0000000021 1 0 2024-07-25 11:23:49 (SEC	-05:00 0000012091
	3 2024-07-2	5 10:30:00.559293	10.201.231.67	10.201.231.90	Syslog	385	Local 6. NOTICE: Jul 25 11:30:00 SSPT33A CELE Administrative and Operational Audit 0000000022 1 0 2024-07-25 11:30:00 558	-05:00 0000012893
	4 2024-07-2	5 10:31:12.796473	10.201.231.67	10.201.231.90	Syslog	423	LOCALG.NOTICE: Jul 25 11:31:12 SSPT33A CISE Administrative and Operational Audit 0000000023 1 0 2024-07-25 11:31:12.796	-05:00 0000012895
	5 2024-07-2	5 10:32:01.217780	10.201.231.90	10.201.231.95	BROWSER	243	Host Announcement DESKTOP-J6CKUCC, Workstation, Server, SQL Server, NT Workstation	
	6 2024-07-2	5 10:32:10.383530	10.201.231.67	10.201.231.90	Syslog	520	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000024 1 0 2024-07-25 11:32:10.382	-05:00 0000012896 !
	7 2024-07-2	5 10:32:10.383668	3 10.201.231.67	10.201.231.90	Syslog	519	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000025 1 0 2024-07-25 11:32:10.383	-05:00 0000012897 !
	8 2024-07-2	5 10:32:10.383760	10.201.231.67	10.201.231.90	Syslog	516	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 000000026 1 0 2024-07-25 11:32:10.383	-05:00 0000012898 5
	9 2024-07-2	5 10:32:10.383807	10.201.231.67	10.201.231.90	Syslog	516	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000027 1 0 2024-07-25 11:32:10.383	-05:00 0000012899 !
	10 2024-07-2	5 10:32:10.383878	3 10.201.231.67	10.201.231.90	Syslog	528	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000028 1 0 2024-07-25 11:32:10.383	-05:00 0000012900 !
	11 2024-07-2	5 10:32:10.383945	5 10.201.231.67	10.201.231.90	Syslog	517	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000029 1 0 2024-07-25 11:32:10.383	-05:00 0000012901 !
	12 2024-07-2	5 10:32:10.384053	3 10.201.231.67	10.201.231.90	Syslog	505	LOCAL6.NOTICE: Jul 25 11:32:10 SSPT33A CISE_Administrative_and_Operational_Audit 0000000000 1 0 2024-07-25 11:32:10.383	-05:00 0000012902 5
_								_
> Frame	e 1: 385 byte	s on wire (3080 b	oits), 385 bytes (aptured (3080 bits)	100.50.55.	5.05.96)		
Toter	rnet II, Src:	Version 4 Src:	10 201 221 67 0	12), DSC: VMWare_a5:65:80	(00:50:50:6	ap:ep:80)		
liser	Datagram Pro	tocol. Src Port:	32724. Dst Port:	514				
 Itru 	uncated]Svslo	a message: LOCALE	5.NOTICE: Jul 25 1	11:29:37 SSPT33A CISE Adm	inistrative	and Operation	al Audit 000000020 1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged	off. ConfigVersion
10	11 0 = Fa	cility: LOCAL6 -	reserved for loca	l use (22)				,
	101 = Le	vel: NOTICE - nor	mal but significa	nt condition (5)				
∨ Me	ssage [trunca	ated]: Jul 25 11:	29:37 SSPT33A CIS	E_Administrative_and_Ope	ational_Aud	it 0000000020	1 0 2024-07-25 11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersionI	d=285, AdminInterf
	Syslog times	tamp (RFC3164): 3	Jul 25 11:29:37					
	Syslog hostm	ame: SSPT33A						
	Syslog proce	ss id: CISE						
	Syslog messa	ge id [truncated]]: _Administrative	e_and_Operational_Audit 0	000000020 1	0 2024-07-25	11:29:37.234 -05:00 0000012891 51002 NOTICE Administrator-Login: Administrator logged off, ConfigVersionId=285, AdminInte	erface=GUI, AdminIP

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).