

Aggiornare il gateway di difesa multicolore dal controller di difesa multicolore

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Aggiornamento di Multicast Defense Gateway](#)

[Verifica](#)

[Monitorare il processo di aggiornamento dall'elenco Gategay.](#)

[Monitorare il processo gateway dai registri di sistema.](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive il processo di aggiornamento di Multicast Defense Gateway da Multicast Defense Controller.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Controller difesa multicolore
- Multicast Defense Gateway

Componenti usati

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

- Multicast Defense Gateway versione 23.08-14.

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

Il processo di upgrade non ha alcun impatto operativo o tempi di inattività. Multicast Defense Controller crea un nuovo set di istanze con la nuova versione dell'immagine. Quando le nuove istanze sono disponibili, il gateway inizia a elaborare il traffico. Una volta scaricato il traffico sulle vecchie istanze, le vecchie istanze vengono eliminate.

Configurazione

Aggiornamento di Multicast Defense Gateway

Le immagini seguenti mostrano il processo di aggiornamento di Multicast Defense Gateway. Il processo di aggiornamento del gateway in ingresso e in uscita è lo stesso.

1. Accedere innanzitutto al controller della difesa multicolore e passare a **Manage > Gateways**.

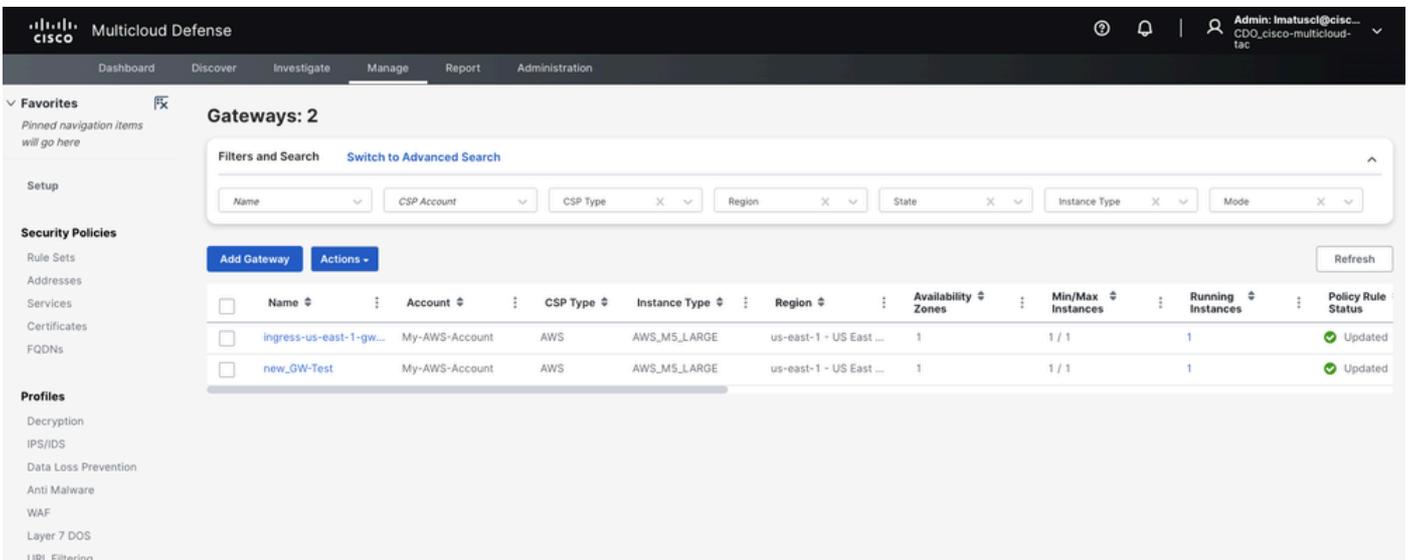


Immagine 1. Elenco gateway.

2. Identificare e selezionare il gateway da aggiornare. È possibile effettuare una sola selezione alla volta.

The screenshot displays the Cisco Multicloud Defense interface. On the left, a sidebar contains navigation menus for Favorites, Security Policies, and Profiles. The main area is titled "Gateways: 2" and includes a "Filters and Search" section. Below this, a table lists gateways with columns for Name and Account. The gateway "ingress-us-east-1-gw-01" is highlighted with a red box. To the right, the "Details" panel for this gateway is shown, with the "Name" field also highlighted in red. The details include fields for State (ACTIVE), Description, Instance Type (AWS_M5_LARGE), Min/Max Instances (1 / 1), Mode (HUB / Ingress), Policy Rule Set (cisco-cd-sample-ingress-policy-ruleset), Gateway Endpoint, Image, Packet Capture Profile, Log Profile, Metrics Profile, NTP Profile, and BGP Profile. At the top of the details panel, there are buttons for "Edit", "Send Diagnostics", "Upgrade", and "Abort". The "Upgrade" button is highlighted with a red box.

Immagine 2. Dettagli del gateway.

3.a. Effettuare la selezione **Upgrade** dalla finestra dei dettagli del gateway.

This screenshot is similar to the previous one, showing the same gateway details. However, the "Upgrade" button in the top right of the details panel is now highlighted with a red box, indicating the next step in the process.

Immagine 3. È possibile aggiornare il gateway dalla scheda dei dettagli.

3.b. È inoltre possibile selezionare **Actions > Upgrade**.

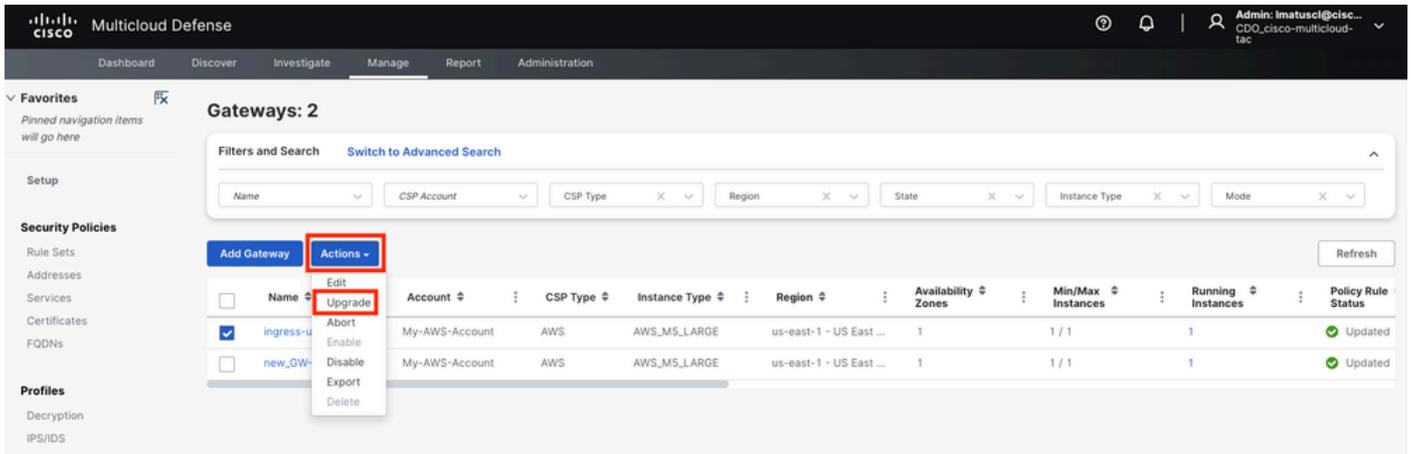


Immagine 4. È possibile aggiornare il gateway tramite il pulsante Azione.

4. Selezionare il menu a discesa per visualizzare le versioni dei gateway disponibili. Quindi, selezionare la versione di destinazione e salvare le modifiche.

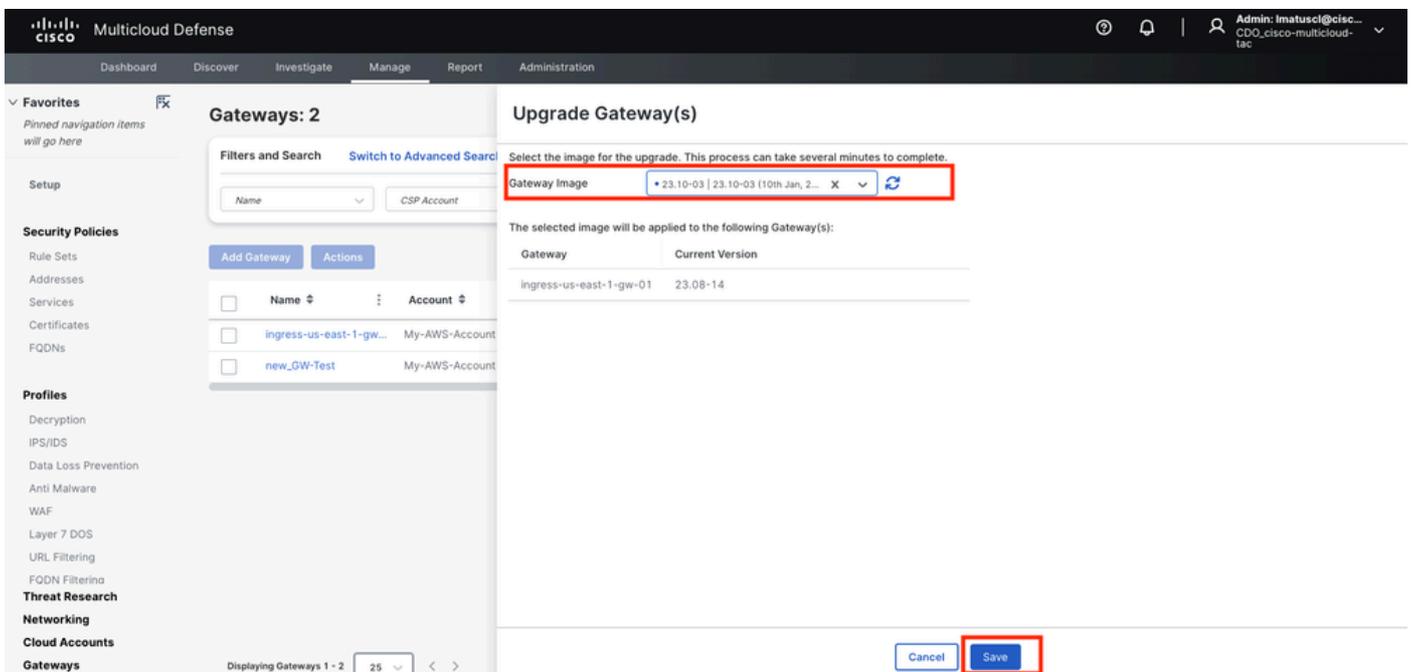


Immagine 5. Versioni disponibili del gateway.

Confermare l'allocazione di risorse del provider di servizi cloud necessaria per l'aggiornamento.

6. Selezionare **Yes** se l'allocazione delle risorse è sufficiente. Fare clic su **No** se l'allocazione delle risorse è insufficiente, aumentare l'allocazione delle risorse nel provider di servizi cloud e tornare a continuare l'aggiornamento.

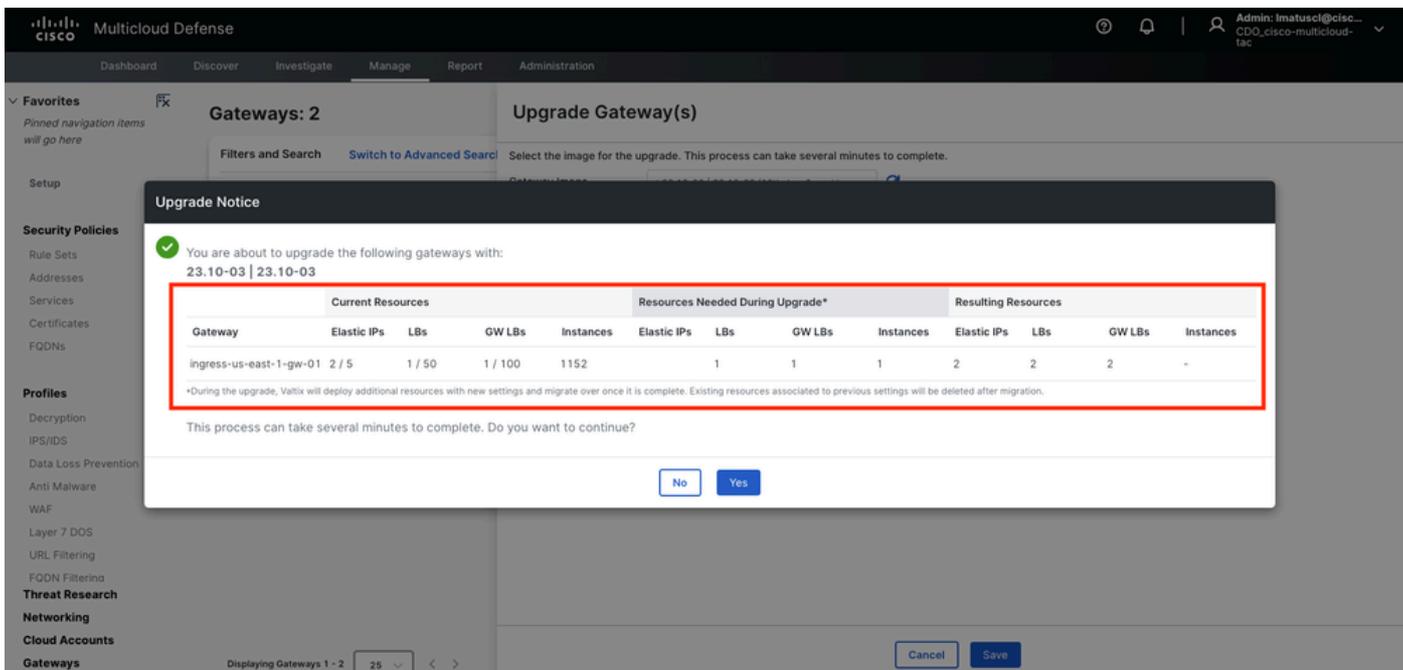


Immagine 6. Allocazione delle risorse nel provider di servizi cloud.

Verifica

Monitorare il processo di aggiornamento dall'elenco Gateway.

Il completamento del processo può richiedere diversi minuti. È possibile monitorare il processo dalla pagina elenco gateway.

Passare a Manage > Gateways.

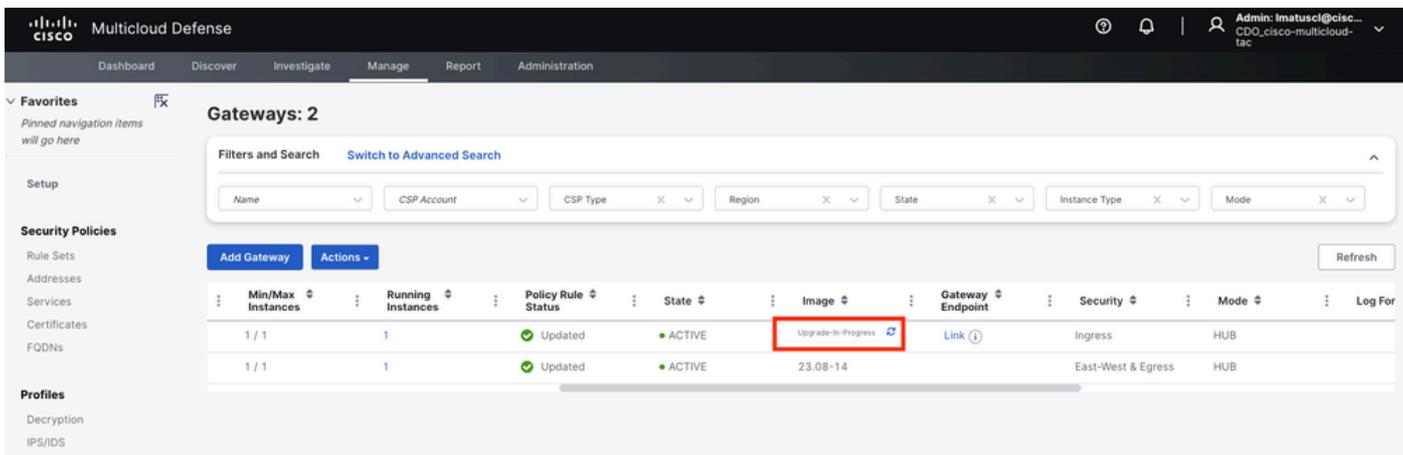


Immagine 7. Pulsante Aggiorna per monitorare il processo di aggiornamento.

Al termine del processo di aggiornamento, il gateway visualizza la nuova versione.

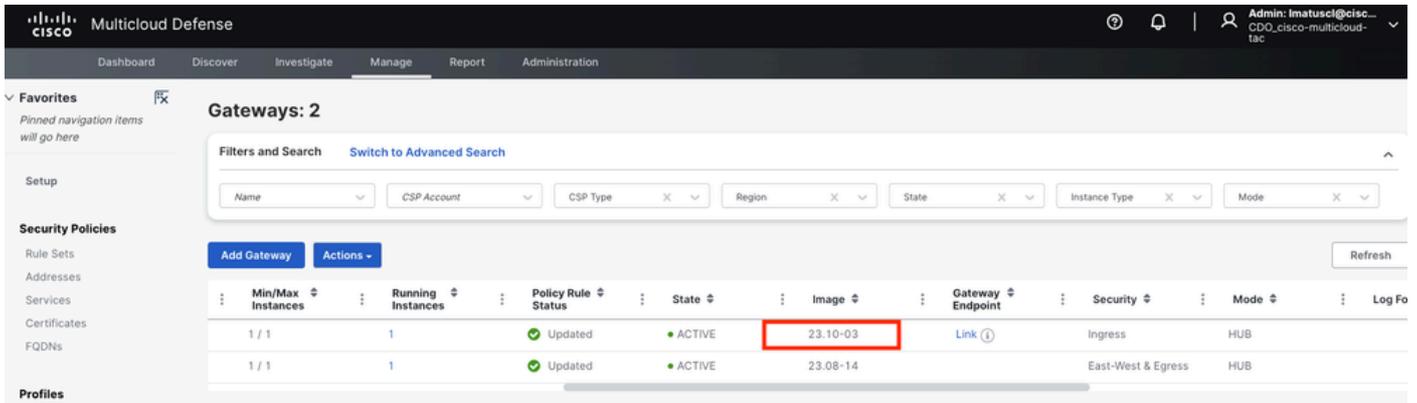


Immagine 8. Processo di aggiornamento completato.

Monitorare il processo gateway dai registri di sistema.

Passare a Investigate > System Logs.

È possibile visualizzare la data e l'ora di inizio e di completamento del processo di aggiornamento.

Selezionare questa opzione **more** per visualizzare ulteriori informazioni sui registri di sistema.

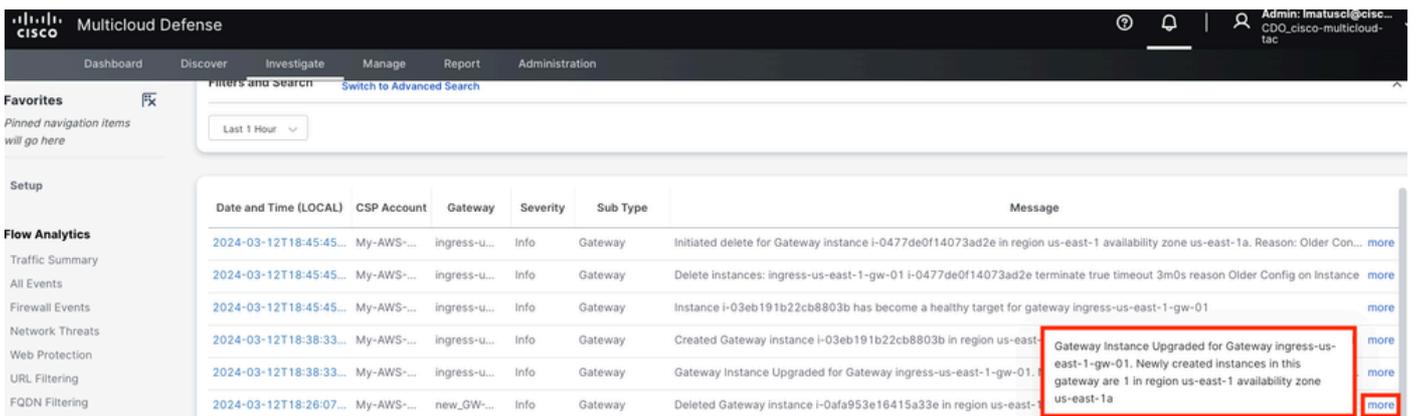


Immagine 9. Log di sistema.

In questa immagine viene mostrato come nei log di sistema viene visualizzata la creazione della nuova istanza del gateway e l'eliminazione di quella precedente quando quella nuova è integra e pronta.

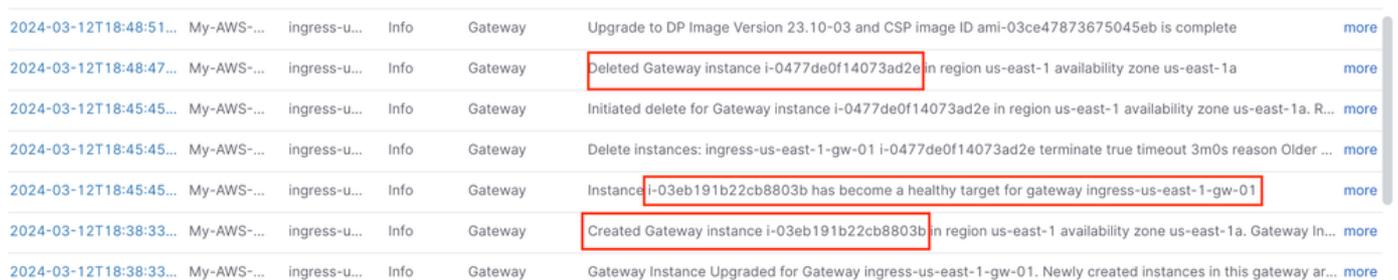


Immagine 10. Creazione ed eliminazione della vecchia e della nuova istanza.

In questa immagine vengono mostrati tutti i log di sistema correlati al processo di aggiornamento del gateway.

System Logs

Filters and Search [Switch to Advanced Search](#)

Last 1 Hour

Date and Time (LOCAL)	CSP Account	Gateway	Severity	Sub Type	Message
2024-03-12T18:48:51...	My-AWS...	ingress-u...	Info	Gateway	Upgrade to DP Image Version 23.10-03 and CSP image ID ami-03ce47873675045eb is complete
2024-03-12T18:48:47...	My-AWS...	ingress-u...	Info	Gateway	Deleted Gateway instance i-0477de0f14073ad2e in region us-east-1 availability zone us-east-1a
2024-03-12T18:45:45...	My-AWS...	ingress-u...	Info	Gateway	Initiated delete for Gateway instance i-0477de0f14073ad2e in region us-east-1 availability zone us-east-1a. Reason: Older Config on Insta...
2024-03-12T18:45:45...	My-AWS...	ingress-u...	Info	Gateway	Delete instances: ingress-us-east-1-gw-01 i-0477de0f14073ad2e terminate true timeout 3m0s reason Older Config on Instance
2024-03-12T18:45:45...	My-AWS...	ingress-u...	Info	Gateway	Instance i-03eb191b22cb8803b has become a healthy target for gateway ingress-us-east-1-gw-01
2024-03-12T18:38:33...	My-AWS...	ingress-u...	Info	Gateway	Created Gateway instance i-03eb191b22cb8803b in region us-east-1 availability zone us-east-1a. Gateway Instance Upgraded
2024-03-12T18:38:33...	My-AWS...	ingress-u...	Info	Gateway	Gateway Instance Upgraded for Gateway ingress-us-east-1-gw-01. Newly created instances in this gateway are 1 in region us-east-1 avail...

Immagine 11. Registri di sistema correlati al processo di aggiornamento del gateway.

Informazioni correlate

- [Guida per l'utente di Cisco Multicast Defense](#)
- [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).