



Gestire il bilanciamento del carico

StorageGRID

NetApp
April 10, 2024

Sommario

- Gestire il bilanciamento del carico 1
 - Gestire il bilanciamento del carico: Panoramica 1
 - Come funziona il bilanciamento del carico - Servizio di bilanciamento del carico 1
 - Configurare gli endpoint del bilanciamento del carico 2
 - Come funziona il bilanciamento del carico - servizio CLB (obsoleto) 10

Gestire il bilanciamento del carico

Gestire il bilanciamento del carico: Panoramica

È possibile utilizzare le funzioni di bilanciamento del carico di StorageGRID per gestire i carichi di lavoro di acquisizione e recupero dai client S3 e Swift. Il bilanciamento del carico massimizza la velocità e la capacità di connessione distribuendo i carichi di lavoro e le connessioni tra più nodi di storage.

Puoi bilanciare il carico dei carichi di lavoro dei client nei seguenti modi:

- Utilizzare il servizio Load Balancer, installato nei nodi Admin e nei nodi Gateway. Il servizio Load Balancer fornisce il bilanciamento del carico di livello 7 ed esegue la terminazione TLS delle richieste dei client, ispeziona le richieste e stabilisce nuove connessioni sicure ai nodi di storage. Si tratta del meccanismo di bilanciamento del carico consigliato.

Vedere [Come funziona il bilanciamento del carico - Servizio di bilanciamento del carico](#).

- Utilizzare il servizio di bilanciamento del carico di connessione (CLB) obsoleto, installato solo sui nodi gateway. Il servizio CLB fornisce il bilanciamento del carico di livello 4 e supporta i costi di collegamento.

Vedere [Come funziona il bilanciamento del carico - servizio CLB \(obsoleto\)](#).

- Integrare un bilanciamento del carico di terze parti. Per ulteriori informazioni, contatta il tuo account rappresentante NetApp.

Come funziona il bilanciamento del carico - Servizio di bilanciamento del carico

Il servizio Load Balancer distribuisce le connessioni di rete in entrata dalle applicazioni client ai nodi di storage. Per abilitare il bilanciamento del carico, è necessario configurare gli endpoint del bilanciamento del carico utilizzando Grid Manager.

È possibile configurare gli endpoint del bilanciamento del carico solo per i nodi Admin o Gateway, poiché questi tipi di nodi contengono il servizio Load Balancer. Non è possibile configurare gli endpoint per i nodi di storage o i nodi di archiviazione.

Ogni endpoint del bilanciamento del carico specifica una porta, un protocollo di rete (HTTP o HTTPS), un tipo di client (S3 o Swift) e una modalità di binding. Gli endpoint HTTPS richiedono un certificato server. Le modalità di binding consentono di limitare l'accessibilità delle porte degli endpoint a:

- Gli indirizzi IP virtuali (VIP) di specifici gruppi ad alta disponibilità (ha)
- Interfacce di rete specifiche di nodi Admin e Gateway specifici

Considerazioni sulle porte

I client possono accedere a qualsiasi endpoint configurato su qualsiasi nodo che esegue il servizio Load Balancer, con due eccezioni: Le porte 80 e 443 sono riservate sui nodi di amministrazione, in modo che gli endpoint configurati su queste porte supportino le operazioni di bilanciamento del carico solo sui nodi gateway.

Se sono state rimappate delle porte, non è possibile utilizzare le stesse porte per configurare gli endpoint del bilanciamento del carico. È possibile creare endpoint utilizzando porte rimappate, ma tali endpoint verranno rimappati alle porte e al servizio CLB originali, non al servizio Load Balancer. Seguire la procedura descritta in [Rimuovere i rimap delle porte](#).



Il servizio CLB è obsoleto.

Disponibilità della CPU

Il servizio Load Balancer su ciascun nodo Admin e nodo Gateway opera in modo indipendente quando inoltra il traffico S3 o Swift ai nodi Storage. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai nodi di storage con una maggiore disponibilità della CPU. Le informazioni sul carico della CPU del nodo vengono aggiornate ogni pochi minuti, ma la ponderazione potrebbe essere aggiornata più frequentemente. A tutti i nodi di storage viene assegnato un valore minimo di peso di base, anche se un nodo riporta un utilizzo pari al 100% o non ne riporta l'utilizzo.

In alcuni casi, le informazioni sulla disponibilità della CPU sono limitate al sito in cui si trova il servizio Load Balancer.

Configurare gli endpoint del bilanciamento del carico

Gli endpoint del bilanciamento del carico determinano le porte e i protocolli di rete che i client S3 e Swift possono utilizzare per la connessione al bilanciamento del carico StorageGRID sui nodi gateway e di amministrazione.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un [browser web supportato](#).
- Si dispone dell'autorizzazione di accesso root.
- Se in precedenza è stata rimappata una porta che si intende utilizzare per l'endpoint del bilanciamento del carico, è possibile [rimosso il remap della porta](#).
- Hai creato tutti i gruppi ad alta disponibilità (ha) che intendi utilizzare. I gruppi HA sono consigliati, ma non richiesti. Vedere [Gestire i gruppi ad alta disponibilità](#).
- Se l'endpoint del bilanciamento del carico verrà utilizzato da [S3 tenant per S3 Select](#), Non deve utilizzare gli indirizzi IP o FQDN di nodi bare-metal. Solo le appliance SG100 o SG1000 e i nodi software basati su VMware sono consentiti per gli endpoint del bilanciamento del carico utilizzati per S3 Select.
- Sono state configurate le interfacce VLAN che si intende utilizzare. Vedere [Configurare le interfacce VLAN](#).
- Se si crea un endpoint HTTPS (consigliato), si dispone delle informazioni per il certificato del server.



Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

- Per caricare un certificato, è necessario disporre del certificato del server, della chiave privata del certificato e, facoltativamente, di un bundle CA.
- Per generare un certificato, sono necessari tutti i nomi di dominio e gli indirizzi IP utilizzati dai client S3 o Swift per accedere all'endpoint. Devi anche conoscere l'oggetto (Nome distinto).
- Se si desidera utilizzare il certificato API StorageGRID S3 e Swift (che può essere utilizzato anche per le connessioni dirette ai nodi di storage), il certificato predefinito è già stato sostituito con un certificato personalizzato firmato da un'autorità di certificazione esterna. Vedere [Configurare i certificati API S3 e](#)

Swift.

Il certificato può utilizzare i caratteri jolly per rappresentare i nomi di dominio completi di tutti i nodi Admin e Gateway che eseguono il servizio Load Balancer. Ad esempio, *.storagegrid.example.com utilizza il carattere jolly * per rappresentare adm1.storagegrid.example.com e gn1.storagegrid.example.com. Vedere [Configurare i nomi di dominio degli endpoint API S3](#).

Creare un endpoint per il bilanciamento del carico

Ogni endpoint del bilanciamento del carico specifica una porta, un tipo di client (S3 o Swift) e un protocollo di rete (HTTP o HTTPS).

Accedere alla procedura guidata

1. Selezionare **CONFIGURATION > Network > Load Balancer Endpoints**.
2. Selezionare **Crea**.

Inserire i dettagli dell'endpoint

1. Inserire i dettagli per l'endpoint.

Create a load balancer endpoint

1 Enter endpoint details

2 Select binding mode

3 Attach certificate

Endpoint details

Name ?

Port ?

Enter an unused port or accept the suggested port.

10443

Client type ?

Select the type of client application that will use this endpoint.

☒ S3 ☐ Swift

Network protocol ?

Select the network protocol clients will use with this endpoint. If you select HTTPS, attach the security certificate before saving the endpoint.

☐ HTTPS (recommended) ☒ HTTP

Cancel

Continue

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella della pagina endpoint del bilanciamento del carico.
Porta	<p>I client delle porte utilizzeranno per connettersi al servizio Load Balancer sui nodi Admin e sui nodi Gateway.</p> <p>Accettare il numero di porta consigliato o inserire una porta esterna non utilizzata da un altro servizio di rete. Inserire un valore compreso tra 1 e 65535.</p> <p>Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway. Queste porte sono riservate sui nodi di amministrazione.</p> <p>Vedere Linee guida per il networking per informazioni sulle porte esterne.</p>
Tipo di client	Il tipo di applicazione client che utilizzerà questo endpoint, S3 o Swift .
Protocollo di rete	<p>Il protocollo di rete che i client utilizzeranno per la connessione a questo endpoint.</p> <ul style="list-style-type: none"> • Selezionare HTTPS per la comunicazione sicura con crittografia TLS (scelta consigliata). È necessario allegare un certificato di sicurezza prima di poter salvare l'endpoint. • Selezionare HTTP per comunicazioni meno sicure e non crittografate. Utilizzare HTTP solo per una griglia non di produzione.

2. Selezionare **continua**.

Selezionare la modalità di binding

1. Selezionare una modalità di binding per l'endpoint per controllare le modalità di accesso all'endpoint.

Opzione	Descrizione
Globale (impostazione predefinita)	<p>I client possono accedere all'endpoint utilizzando un FQDN (Fully Qualified Domain Name), l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore o l'indirizzo IP virtuale di qualsiasi gruppo su qualsiasi rete.</p> <p>Utilizzare l'impostazione Global (predefinita) a meno che non sia necessario limitare l'accessibilità di questo endpoint.</p>
Interfacce di nodo	I client devono utilizzare l'indirizzo IP di un nodo e di un'interfaccia di rete selezionati per accedere a questo endpoint.

Opzione	Descrizione
IP virtuali dei gruppi ha	<p>I client devono utilizzare un indirizzo IP virtuale di un gruppo ha per accedere a questo endpoint.</p> <p>Gli endpoint con questa modalità di binding possono utilizzare tutti lo stesso numero di porta, purché i gruppi ha selezionati per gli endpoint non si sovrappongano.</p> <p>Gli endpoint con questa modalità possono utilizzare tutti lo stesso numero di porta purché le interfacce selezionate per gli endpoint non si sovrappongano.</p>



Se si utilizza la stessa porta per più di un endpoint, un endpoint che utilizza la modalità **Virtual IP of ha groups** sovrascrive un endpoint utilizzando la modalità **Node interfaces**, che sovrascrive un endpoint utilizzando la modalità **Global**.

- Se si seleziona **Node interfaces**, selezionare una o più interfacce di nodo per ciascun nodo Admin o nodo gateway che si desidera associare a questo endpoint.

Binding mode ?

Select a binding mode if you plan to monitor or limit the use of this endpoint with a traffic classification policy.

The binding mode controls how the endpoint is accessed—using any IP address or using specific IP addresses and network interfaces.

☐ Global
 ☒ Node interfaces
 ☐ Virtual IPs of HA groups

If you use the same port for more than one endpoint, an endpoint bound to HA groups overrides an endpoint bound to Node interfaces, which overrides a Global endpoint. If this behavior does not meet your requirements, consider using a different port number for each endpoint.

Total interface count: 3

<input type="checkbox"/>	Node ?	Node interface ?	Site ?	IP address ?	Node type ?
<input type="checkbox"/>	DC1-ADM1	eth0 ?	Data Center 1	172.16.3.246 and 2 more	Primary Admin Node
<input type="checkbox"/>	DC1-ADM1	eth1 ?	Data Center 1	10.224.3.246 and 5 more	Primary Admin Node
<input type="checkbox"/>	DC1-ADM1	eth2 ?	Data Center 1	47.47.3.246 and 3 more	Primary Admin Node

- Se si seleziona **IP virtuali dei gruppi ha**, selezionare uno o più gruppi ha.


Binding mode ?

Select a binding mode if you plan to monitor or limit the use of this endpoint with a traffic classification policy.

The binding mode controls how the endpoint is accessed—using any IP address or using specific IP addresses and network interfaces.

☐ Global ☐ Node interfaces ☒ Virtual IPs of HA groups

If you use the same port for more than one endpoint, an endpoint bound to HA groups overrides an endpoint bound to Node interfaces, which overrides a Global endpoint. If this behavior does not meet your requirements, consider using a different port number for each endpoint.



Total interface count: 2

<input type="checkbox"/>	Name ?	Description ?	Virtual IP address ?	Interfaces (in priority order) ?
<input type="checkbox"/>	FabricPool	Use for FabricPool client access	10.96.104.5 10.96.104.6	DC1-ADM1-104-96:eth2 (active) DC2-ADM1-104-103:eth2
<input type="checkbox"/>	S3 Clients	use for S3 client access	10.96.104.10	DC1-ADM1-104-96:eth0 DC2-ADM1-104-103:eth0

4. Se si crea un endpoint **HTTP**, non è necessario allegare un certificato. Selezionare **Create** per aggiungere il nuovo endpoint del bilanciamento del carico. Quindi, passare a [Al termine](#). In caso contrario, selezionare **continua** per allegare il certificato.

Allega certificato

1. Se si sta creando un endpoint **HTTPS**, selezionare il tipo di certificato di sicurezza che si desidera allegare all'endpoint.

Il certificato protegge le connessioni tra i client S3 e Swift e il servizio Load Balancer sui nodi Admin Node o Gateway.

- **Carica certificato.** Selezionare questa opzione se si dispone di certificati personalizzati da caricare.
- **Genera certificato.** Selezionare questa opzione se si dispone dei valori necessari per generare un certificato personalizzato.
- **Utilizzare il certificato StorageGRID S3 e Swift.** Selezionare questa opzione se si desidera utilizzare il certificato globale S3 e Swift API, che può essere utilizzato anche per le connessioni dirette ai nodi di storage.

Non è possibile selezionare questa opzione a meno che non sia stato sostituito il certificato S3 e Swift API predefinito, firmato dalla CA Grid, con un certificato personalizzato firmato da un'autorità di certificazione esterna. Vedere [Configurare i certificati API S3 e Swift](#).

2. Se non si utilizza il certificato StorageGRID S3 e Swift, caricare o generare il certificato.

Carica certificato

- a. Selezionare **carica certificato**.
- b. Caricare i file dei certificati del server richiesti:
 - **Server certificate**: Il file di certificato del server personalizzato in codifica PEM.
 - **Certificate private key** (chiave privata certificato): Il file di chiave privata del certificato del server personalizzato (.key).



Le chiavi private EC devono essere 224 bit o superiori. Le chiavi private RSA devono essere 2048 bit o superiori.

- **Bundle CA**: Un singolo file opzionale contenente i certificati di ogni autorità di certificazione di emissione intermedia (CA). Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.
- c. Espandere **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.
 - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.
- d. Selezionare **Crea**. + viene creato l'endpoint del bilanciamento del carico. Il certificato personalizzato viene utilizzato per tutte le nuove connessioni successive tra i client S3 e Swift e l'endpoint.

Generare un certificato

- a. Selezionare **genera certificato**.
- b. Specificare le informazioni del certificato:
 - **Domain name**: Uno o più nomi di dominio completi da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.
 - **IP**: Uno o più indirizzi IP da includere nel certificato.
 - **Oggetto**: Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
 - **Giorni validi**: Numero di giorni successivi alla creazione della scadenza del certificato.
- c. Selezionare **generate**.
- d. Selezionare **Dettagli certificato** per visualizzare i metadati del certificato generato.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Crea**.

Viene creato l'endpoint del bilanciamento del carico. Il certificato personalizzato viene utilizzato per tutte le nuove connessioni successive tra i client S3 e Swift e questo endpoint.

[[dopo la fine]]al termine

1. Se si utilizza un sistema di nomi di dominio (DNS), assicurarsi che il DNS includa un record per associare il nome di dominio completo StorageGRID a ciascun indirizzo IP utilizzato dai client per effettuare le connessioni.

L'indirizzo IP inserito nel record DNS dipende dall'utilizzo di un gruppo ha di nodi per il bilanciamento del carico:

- Se è stato configurato un gruppo ha, i client si connetteranno agli indirizzi IP virtuali di quel gruppo ha.
- Se non si utilizza un gruppo ha, i client si connetteranno al servizio bilanciamento del carico StorageGRID utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore.

È inoltre necessario assicurarsi che il record DNS faccia riferimento a tutti i nomi di dominio degli endpoint richiesti, inclusi i nomi con caratteri jolly.

2. Fornire ai client S3 e Swift le informazioni necessarie per connettersi all'endpoint:

- Numero di porta
- Nome di dominio completo o indirizzo IP
- Tutti i dettagli del certificato richiesti

Visualizzare e modificare gli endpoint del bilanciamento del carico

È possibile visualizzare i dettagli degli endpoint del bilanciamento del carico esistenti, inclusi i metadati del certificato per un endpoint protetto. È inoltre possibile modificare il nome o la modalità di binding di un endpoint e aggiornare eventuali certificati associati.

Non è possibile modificare il tipo di servizio (S3 o Swift), la porta o il protocollo (HTTP o HTTPS).

- Per visualizzare le informazioni di base per tutti gli endpoint del bilanciamento del carico, consultare la tabella nella pagina endpoint del bilanciamento del carico.

Create

Actions ▾

Search...

Q

Total endpoints count: 1

<input type="checkbox"/>	Name ? ▾	Port ? ▾	Network protocol ? ▾	Binding mode ? ▾	Certificate expiration ? ▾
<input type="checkbox"/>	FabricPool endpoint	10443	HTTPS	Global	Oct 19th, 2022

- Per visualizzare tutti i dettagli relativi a un endpoint specifico, inclusi i metadati del certificato, selezionare il nome dell'endpoint nella tabella.

FabricPool endpoint

Port: 10443
 Client type: S3
 Network protocol: HTTPS
 Binding mode: Global
 Endpoint ID: c2b6feb3-c567-449d-b717-4fed98c4a411

Remove

Binding Mode

Certificate

You can select a different binding mode or change IP addresses for the current binding mode.

Edit binding mode

Binding mode: Global




This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.

- Per modificare un endpoint, utilizzare il menu **azioni** nella pagina endpoint del bilanciamento del carico o nella pagina dei dettagli di un endpoint specifico.



Dopo aver modificato un endpoint, potrebbe essere necessario attendere fino a 15 minuti per applicare le modifiche a tutti i nodi.

Attività	Menu delle azioni	Pagina dei dettagli
Modificare il nome dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare azioni Modifica nome endpoint . c. Inserire il nuovo nome. d. Selezionare Salva .	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare l'icona di modifica  . c. Inserire il nuovo nome. d. Selezionare Salva .
Modificare la modalità di associazione degli endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare Actions Edit endpoint binding mode . c. Aggiornare la modalità di binding secondo necessità. d. Selezionare Save Changes (Salva modifiche).	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare Edit binding mode (Modifica modalità di associazione). c. Aggiornare la modalità di binding secondo necessità. d. Selezionare Save Changes (Salva modifiche).

Attività	Menu delle azioni	Pagina dei dettagli
Modificare il certificato dell'endpoint	<ul style="list-style-type: none"> a. Selezionare la casella di controllo per l'endpoint. b. Selezionare azioni Modifica certificato endpoint. c. Caricare o generare un nuovo certificato personalizzato o iniziare a utilizzare il certificato globale S3 e Swift, come richiesto. d. Selezionare Save Changes (Salva modifiche). 	<ul style="list-style-type: none"> a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare la scheda certificato. c. Selezionare Modifica certificato. d. Caricare o generare un nuovo certificato personalizzato o iniziare a utilizzare il certificato globale S3 e Swift, come richiesto. e. Selezionare Save Changes (Salva modifiche).

Rimuovere gli endpoint del bilanciamento del carico

È possibile rimuovere uno o più endpoint dal menu **azioni** oppure rimuovere un singolo endpoint dalla pagina dei dettagli.



Per evitare interruzioni del client, aggiornare le applicazioni client S3 o Swift interessate prima di rimuovere un endpoint di bilanciamento del carico. Aggiornare ogni client per la connessione utilizzando una porta assegnata a un altro endpoint del bilanciamento del carico. Assicurarsi di aggiornare anche tutte le informazioni di certificato richieste.

- Per rimuovere uno o più endpoint:
 - a. Dalla pagina bilanciamento del carico, selezionare la casella di controllo per ciascun endpoint che si desidera rimuovere.
 - b. Selezionare **azioni Rimuovi**.
 - c. Selezionare **OK**.
- Per rimuovere un endpoint dalla pagina dei dettagli:
 - a. Dalla pagina bilanciamento del carico, selezionare il nome dell'endpoint.
 - b. Selezionare **Rimuovi** nella pagina dei dettagli.
 - c. Selezionare **OK**.

Come funziona il bilanciamento del carico - servizio CLB (obsoleto)

Il servizio di bilanciamento del carico di connessione (CLB) sui nodi gateway è obsoleto. Il servizio Load Balancer è ora il meccanismo di bilanciamento del carico consigliato.

Il servizio CLB utilizza il bilanciamento del carico di livello 4 per distribuire le connessioni di rete TCP in entrata dalle applicazioni client al nodo di storage ottimale in base alla disponibilità, al carico di sistema e al costo del collegamento configurato dall'amministratore. Quando si sceglie il nodo di storage ottimale, il servizio CLB stabilisce una connessione di rete bidirezionale e inoltra il traffico da e verso il nodo selezionato. La CLB non prende in considerazione la configurazione Grid Network quando indirizza le connessioni di rete in entrata.

Per visualizzare le informazioni sul servizio CLB, selezionare **SUPPORT Tools Grid topology**, quindi

espandere un nodo gateway fino a quando non è possibile selezionare **CLB** e le opzioni sottostanti.

The screenshot displays the StorageGRID WebScale Deployment interface. On the left, the 'Grid Topology' pane shows a hierarchical tree of components. A blue box highlights the 'DC1-G1-98-161' node, which is expanded to show its sub-components: 'SSM', 'CLB', 'HTTP', 'Events', and 'Resources'. The 'CLB' component is selected. On the right, the 'Overview' tab is active, showing a summary for 'DC1-G1-98-161'. The summary includes a 'Storage Capacity' section with a table of metrics.

Storage Capacity		
Storage Nodes Installed:	N/A	
Storage Nodes Readable:	N/A	
Storage Nodes Writable:	N/A	
Installed Storage Capacity:	N/A	
Used Storage Capacity:	N/A	
Used Storage Capacity for Data:	N/A	
Used Storage Capacity for Metadata:	N/A	
Usable Storage Capacity:	N/A	

Se si sceglie di utilizzare il servizio CLB, si consiglia di configurare i costi di collegamento per il sistema StorageGRID.

- [Quali sono i costi di collegamento](#)
- [Aggiornare i costi dei collegamenti](#)

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.