Configurare StorageGRID manualmente

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-117/fabricpool/creating-ha-group-for-fabricpool.html on November 04, 2025. Always check docs.netapp.com for the latest.

Sommario

Configurare StorageGRID manualmente . . . 1
Creare un gruppo ad alta disponibilità (ha) per FabricPool . . . 1
Creare un endpoint di bilanciamento del carico per FabricPool . . . 2
Creare un account tenant per FabricPool . . . 5
Creare un bucket S3 e ottenere le chiavi di accesso . . . 6
Configurare ILM per i dati FabricPool . . . 7
Creare una policy di classificazione del traffico per FabricPool . . . 10

Configurare StorageGRID manualmente

Creare un gruppo ad alta disponibilità (ha) per FabricPool

Quando si configura StorageGRID per l'utilizzo con FabricPool, è possibile creare facoltativamente uno o più gruppi ad alta disponibilità (ha). Un gruppo ha è un insieme di nodi che contengono ciascuno il servizio bilanciamento del carico StorageGRID. Un gruppo ha può contenere nodi gateway, nodi di amministrazione o entrambi.

È possibile utilizzare un gruppo ha per mantenere disponibili le connessioni dati FabricPool. Un gruppo ha utilizza indirizzi IP virtuali (VIP) per fornire un accesso altamente disponibile al servizio Load Balancer. Se l'interfaccia attiva nel gruppo ha si guasta, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni FabricPool.

Per ulteriori informazioni su questa attività, vedere "Gestire i gruppi ad alta disponibilità". Per utilizzare la procedura guidata di installazione di FabricPool per completare questa attività, visitare il sito Web all'indirizzo "Accedere e completare l'installazione guidata di FabricPool".

Prima di iniziare

- Hai esaminato il "best practice per i gruppi ad alta disponibilità".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone dell'autorizzazione di accesso root.
- Se si intende utilizzare una VLAN, è stata creata l'interfaccia VLAN. Vedere "Configurare le interfacce VLAN".

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **High Availability groups**.
2. Selezionare **Crea**.
3. Per la fase **inserire i dettagli**, completare i seguenti campi.

Campo	Descrizione
Nome del gruppo HA	Un nome di visualizzazione univoco per questo gruppo ha.
Descrizione (opzionale)	La descrizione di questo gruppo ha.

4. Per il passo **Add interfaces**, selezionare le interfacce di nodo che si desidera utilizzare in questo gruppo ha.

   Utilizzare le intestazioni di colonna per ordinare le righe o inserire un termine di ricerca per individuare le interfacce più rapidamente.

   È possibile selezionare uno o più nodi, ma è possibile selezionare una sola interfaccia per ciascun nodo.

5. Per la fase **prioritize interfaces**, determinare l'interfaccia primaria e le interfacce di backup per questo gruppo ha.

   Trascinare le righe per modificare i valori nella colonna **Ordine di priorità**.

La prima interfaccia nell'elenco è l'interfaccia primaria. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.

Se il gruppo ha include più di un'interfaccia e l'interfaccia attiva non riesce, gli indirizzi IP virtuali (VIP) si spostano nella prima interfaccia di backup nell'ordine di priorità. Se l'interfaccia non funziona, gli indirizzi VIP passano all'interfaccia di backup successiva e così via. Quando i guasti vengono risolti, gli indirizzi VIP tornano all'interfaccia con la priorità più alta disponibile.

6. Per il passo **inserire gli indirizzi IP**, completare i seguenti campi.

Campo	Descrizione
Subnet CIDR	L'indirizzo della subnet VIP nella notazione CIDR& 8212;un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32). L'indirizzo di rete non deve avere bit host impostati. Ad esempio, `192.16.0.0/22`.
Indirizzo IP del gateway (opzionale)	Opzionale. Se gli indirizzi IP ONTAP utilizzati per accedere a StorageGRID non si trovano sulla stessa sottorete degli indirizzi VIP StorageGRID, immettere l'indirizzo IP del gateway locale VIP StorageGRID. L'indirizzo IP del gateway locale deve trovarsi all'interno della subnet VIP.
Virtual IP address (Indirizzo IP virtuale)	Inserire almeno uno e non più di dieci indirizzi VIP per l'interfaccia attiva nel gruppo ha. Tutti gli indirizzi VIP devono trovarsi all'interno della subnet VIP. Almeno un indirizzo deve essere IPv4. In alternativa, è possibile specificare ulteriori indirizzi IPv4 e IPv6.

7. Selezionare **Create ha group** (Crea gruppo ha), quindi selezionare **Finish** (fine).

Creare un endpoint di bilanciamento del carico per FabricPool

StorageGRID utilizza un bilanciamento del carico per gestire il carico di lavoro dalle applicazioni client, come FabricPool. Il bilanciamento del carico massimizza la velocità e la capacità di connessione tra più nodi di storage.

Quando si configura StorageGRID per l'utilizzo con FabricPool, è necessario configurare un endpoint di bilanciamento del carico e caricare o generare un certificato endpoint di bilanciamento del carico, utilizzato per proteggere la connessione tra ONTAP e StorageGRID.

Per utilizzare la procedura guidata di installazione di FabricPool per completare questa attività, visitare il sito Web all'indirizzo "Accedere e completare l'installazione guidata di FabricPool".

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone dell'autorizzazione di accesso root.

- Hai esaminato il generale "considerazioni per il bilanciamento del carico" così come il "Best practice per il bilanciamento del carico per FabricPool".

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **Load Balancer Endpoints**.
2. Selezionare **Crea**.
3. Per il passo **inserire i dettagli dell'endpoint**, completare i seguenti campi.

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint.
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è 10433 per il primo endpoint creato, ma è possibile inserire qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway. Queste porte sono riservate sui nodi di amministrazione. **Nota:** le porte utilizzate da altri servizi di rete non sono consentite. Vedere"Riferimento porta di rete". Fornirai questo numero a ONTAP quando Aggiungi StorageGRID come Tier cloud FabricPool.
Tipo di client	Selezionare **S3**.
Protocollo di rete	Selezionare **HTTPS**. **Nota**: La comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

4. Per il passo **Select binding mode**, specificare la modalità di binding. La modalità di binding controlla il modo in cui si accede all'endpoint utilizzando qualsiasi indirizzo IP o indirizzi IP e interfacce di rete specifici. 8212

Opzione	Descrizione
Globale (impostazione predefinita)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione **Global** (predefinita) a meno che non sia necessario limitare l'accessibilità di questo endpoint.

Opzione	Descrizione
IP virtuali dei gruppi ha	Per accedere a questo endpoint, i client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha. 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.
Interfacce di nodo	I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate per accedere a questo endpoint.
Tipo di nodo	In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway per accedere a questo endpoint.

5. Per il passaggio **accesso tenant**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Allow all tenant (Consenti tutti i tenant) (impostazione predefinita	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai bucket. **Allow all tenant** è quasi sempre l'opzione appropriata per l'endpoint di bilanciamento del carico utilizzato per FabricPool. Selezionare questa opzione se non sono ancora stati creati account tenant.
Consenti tenant selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai bucket.
Blocca i tenant selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

6. Per il passo **Allega certificato**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Carica certificato (consigliato)	Utilizzare questa opzione per caricare un certificato server firmato dalla CA, una chiave privata del certificato e un bundle CA opzionale.
Generare un certificato	Utilizzare questa opzione per generare un certificato autofirmato. Vedere "Configurare gli endpoint del bilanciamento del carico" per informazioni dettagliate su cosa inserire.

Campo	Descrizione
Utilizza il certificato StorageGRID S3 e Swift	Questa opzione è disponibile solo se è già stata caricata o generata una versione personalizzata del certificato globale StorageGRID. Vedere "Configurare i certificati API S3 e Swift" per ulteriori informazioni.

7. Selezionare **Crea**.

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

Creare un account tenant per FabricPool

È necessario creare un account tenant in Grid Manager per l'utilizzo con FabricPool.

Gli account tenant consentono alle applicazioni client di memorizzare e recuperare oggetti su StorageGRID. Ogni account tenant dispone di un proprio ID account, gruppi e utenti autorizzati, bucket e oggetti.

Per ulteriori informazioni su questa attività, vedere "Creare un account tenant". Per utilizzare la procedura guidata di installazione di FabricPool per completare questa attività, visitare il sito Web all'indirizzo "Accedere e completare l'installazione guidata di FabricPool".

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **TENANT**.
2. Selezionare **Crea**.
3. Per la procedura di inserimento dei dettagli, immettere le seguenti informazioni.

Campo	Descrizione
Nome	Un nome per l'account tenant. I nomi dei tenant non devono essere univoci. Una volta creato, l'account tenant riceve un ID account numerico univoco.
Descrizione (opzionale)	Una descrizione che aiuta a identificare il tenant.
Tipo di client	Deve essere **S3** per FabricPool.
Quota di storage (opzionale)	Lasciare vuoto questo campo per FabricPool.

4. Per il passo Select permissions:
   a. Non selezionare **Allow platform Services** (Consenti servizi piattaforma).

      I tenant FabricPool non devono in genere utilizzare servizi di piattaforma, come la replica di

CloudMirror.

b. Facoltativamente, selezionare **Usa origine identità propria**.

c. Non selezionare **Allow S3 Select** (Consenti selezione S3).

I tenant FabricPool in genere non devono utilizzare S3 Select.

d. Facoltativamente, selezionare **Usa connessione federazione griglia** per consentire al tenant di utilizzare un "connessione a federazione di griglie" per il clone dell'account e la replica cross-grid. Quindi, selezionare la connessione a federazione di griglie da utilizzare.

5. Per la fase di definizione dell'accesso root, specificare quale utente disporrà dell'autorizzazione di accesso root iniziale per l'account tenant, a seconda che il sistema StorageGRID utilizzi o meno "federazione delle identità", "SSO (Single Sign-on)", o entrambi.

Opzione	Eseguire questa operazione
Se la federazione delle identità non è attivata	Specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se è attivata la federazione delle identità	a. Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se sono attivate sia la federazione di identità che il single sign-on (SSO)	Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. Nessun utente locale può accedere.

6. Selezionare **Crea tenant**.

Creare un bucket S3 e ottenere le chiavi di accesso

Prima di utilizzare StorageGRID con un carico di lavoro FabricPool, è necessario creare un bucket S3 per i dati FabricPool. È inoltre necessario ottenere una chiave di accesso e una chiave di accesso segreta per l'account tenant che si utilizzerà per FabricPool.

Per ulteriori informazioni su questa attività, vedere "Creare un bucket S3" e. "Creare le proprie chiavi di accesso S3". Per utilizzare la procedura guidata di installazione di FabricPool per completare questa attività, visitare il sito Web all'indirizzo "Accedere e completare l'installazione guidata di FabricPool".

Prima di iniziare

- È stato creato un account tenant per l'utilizzo di FabricPool.
- Si dispone dell'accesso root all'account tenant.

Fasi

1. Accedi al tenant manager.

È possibile effettuare una delle seguenti operazioni:

- Dalla pagina account tenant in Grid Manager, selezionare il collegamento **Accedi** per il tenant e immettere le credenziali.
- Immettere l'URL dell'account tenant in un browser Web e le credenziali.

2. Creare un bucket S3 per i dati FabricPool.

   È necessario creare un bucket unico per ogni cluster ONTAP che si intende utilizzare.

   a. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3)** > **Bucket**.
   b. Selezionare **Crea bucket**.
   c. Immettere il nome del bucket StorageGRID che si desidera utilizzare con FabricPool. Ad esempio, `fabricpool-bucket`.

      Non è possibile modificare il nome del bucket dopo averlo creato.

   d. Selezionare la regione per questo bucket.

      Per impostazione predefinita, tutti i bucket vengono creati in `us-east-1` regione.

   e. Selezionare **continua**.
   f. Selezionare **Crea bucket**.

      Non selezionare **attiva versione oggetto** per il bucket FabricPool. Allo stesso modo, non modificare un bucket FabricPool per utilizzare **Available** o un livello di coerenza non predefinito. Il livello di coerenza del bucket consigliato per i bucket FabricPool è **Read-after-new-write**, che è l'impostazione predefinita per un nuovo bucket.

3. Creare una chiave di accesso e una chiave di accesso segreta.

   a. Selezionare **STORAGE (S3)** > **My access key**.
   b. Selezionare **Crea chiave**.
   c. Selezionare **Crea chiave di accesso**.
   d. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in una posizione sicura oppure selezionare **Download .csv** per salvare un foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

      Questi valori verranno immessi in ONTAP quando si configura StorageGRID come livello cloud FabricPool.

      Se in futuro si generano una nuova chiave di accesso e una chiave di accesso segreta in StorageGRID, inserire le nuove chiavi in ONTAP prima di eliminare i vecchi valori da StorageGRID. In caso contrario, ONTAP potrebbe perdere temporaneamente l'accesso a StorageGRID.

Configurare ILM per i dati FabricPool

Puoi utilizzare questo semplice esempio di policy come punto di partenza per le tue regole e policy ILM.

In questo esempio si presuppone che si stiano progettando le regole ILM e una policy ILM per un sistema StorageGRID con quattro nodi di storage in un singolo data center a Denver, Colorado. I dati FabricPool in questo esempio utilizzano un bucket denominato `fabricpool-bucket`.

> Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita. Per ulteriori informazioni, vedere "Gestire gli oggetti con ILM".

> Per evitare la perdita di dati, non utilizzare una regola ILM che scadrà o eliminerà i dati del livello cloud di FabricPool. Impostare il periodo di conservazione su **forever** per garantire che gli oggetti FabricPool non vengano cancellati da ILM StorageGRID.

Prima di iniziare

- Hai esaminato il "Best practice per l'utilizzo di ILM con i dati FabricPool".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone dell'autorizzazione di accesso ILM o Root.
- Se è stato eseguito l'aggiornamento a StorageGRID 11.7 da una versione precedente di StorageGRID, il pool di storage da utilizzare è stato configurato. In generale, è necessario creare un pool di storage per ciascun sito StorageGRID.

> Questo prerequisito non si applica alle nuove installazioni di StorageGRID 11.7. Quando si installa StorageGRID 11.7 su un nuovo grid, i pool di storage vengono creati automaticamente per ciascun sito.

Fasi

1. Creare una regola ILM che si applica solo ai dati in `fabricpool-bucket`. Questa regola di esempio consente di creare copie codificate per la cancellazione.

Definizione della regola	Valore di esempio
Nome della regola	2 + 1 erasure coding per i dati FabricPool
Nome bucket	`fabricpool-bucket` È anche possibile filtrare l'account tenant FabricPool.
Filtri avanzati	Dimensione dell'oggetto superiore a 0.2 MB. **Nota:** FabricPool scrive solo oggetti da 4 MB, ma è necessario aggiungere un filtro per le dimensioni degli oggetti perché questa regola utilizza la codifica di cancellazione.
Tempo di riferimento	Tempo di acquisizione

Definizione della regola	Valore di esempio
Periodo di tempo e collocamenti	Dal giorno 0 memorizzare per sempre Memorizzare gli oggetti cancellando il codice utilizzando lo schema 2+1 EC a Denver e conservarli in StorageGRID per sempre. Per evitare la perdita di dati, non utilizzare una regola ILM che scadrà o eliminerà i dati del livello cloud di FabricPool.
Comportamento di acquisizione	Bilanciato

2. Creare una regola ILM predefinita che crei due copie replicate di qualsiasi oggetto non corrispondente alla prima regola. Non selezionare un filtro di base (account tenant o nome bucket) o filtri avanzati.

Definizione della regola	Valore di esempio
Nome della regola	Due copie replicate
Nome bucket	*nessuno*
Filtri avanzati	*nessuno*
Tempo di riferimento	Tempo di acquisizione
Periodo di tempo e collocamenti	Dal giorno 0 memorizzare per sempre Memorizzare gli oggetti replicando 2 copie a Denver.
Comportamento di acquisizione	Bilanciato

3. Creare una policy ILM proposta e selezionare le due regole. Poiché la regola di replica non utilizza alcun filtro, può essere l'ultima regola predefinita per il criterio.
4. Acquisire oggetti di test nella griglia.
5. Simulare il criterio con gli oggetti di test per verificare il comportamento.
6. Attivare il criterio.

Quando questo criterio è attivato, StorageGRID inserisce i dati degli oggetti come segue:

- I dati a più livelli di FabricPool in `fabricpool-bucket` verrà eseguito un erasure coding utilizzando lo schema di erasure coding 2+1. Due frammenti di dati e un frammento di parità verranno posizionati su tre diversi nodi di storage.
- Tutti gli oggetti in tutti gli altri bucket verranno replicati. Verranno create due copie e collocate su due diversi nodi di storage.
- Le copie verranno conservate in StorageGRID per sempre. ILM di StorageGRID non elimina questi oggetti.

Creare una policy di classificazione del traffico per FabricPool

È possibile, in via opzionale, progettare una policy di classificazione del traffico StorageGRID per ottimizzare la qualità del servizio per il carico di lavoro FabricPool.

Per ulteriori informazioni su questa attività, vedere "Gestire le policy di classificazione del traffico". Per utilizzare la procedura guidata di installazione di FabricPool per completare questa attività, visitare il sito Web all'indirizzo "Accedere e completare l'installazione guidata di FabricPool".

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone dell'autorizzazione di accesso root.

A proposito di questa attività

Le Best practice per la creazione di una policy di classificazione del traffico per FabricPool dipendono dal carico di lavoro, come segue:

- Se si prevede di suddividere i dati del carico di lavoro primario FabricPool in StorageGRID, assicurarsi che il carico di lavoro FabricPool abbia la maggior parte della larghezza di banda. È possibile creare una policy di classificazione del traffico per limitare tutti gli altri carichi di lavoro.

  > In generale, le operazioni di lettura FabricPool sono più importanti per le priorità rispetto alle operazioni di scrittura.

  Ad esempio, se altri client S3 utilizzano questo sistema StorageGRID, è necessario creare un criterio di classificazione del traffico. È possibile limitare il traffico di rete per gli altri bucket, tenant, subnet IP o endpoint del bilanciamento del carico.

*In genere, non è necessario imporre limiti di qualità del servizio su qualsiasi carico di lavoro FabricPool; è necessario limitare solo gli altri carichi di lavoro.

- I limiti imposti agli altri carichi di lavoro devono tenere conto del comportamento di tali carichi di lavoro. I limiti imposti variano anche in base al dimensionamento e alle funzionalità del tuo grid e alla quantità di utilizzo prevista.

Fasi

1. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.
2. Selezionare **Crea**.
3. Inserire un nome e una descrizione (opzionale) per la policy e selezionare **continua**.
4. Per il passo Add Matching rules (Aggiungi regole di corrispondenza), aggiungere almeno una regola.
   a. Selezionare **Aggiungi regola**
   b. Per tipo, selezionare **endpoint del bilanciamento del carico** e selezionare l'endpoint del bilanciamento del carico creato per FabricPool.

      È inoltre possibile selezionare l'account o il bucket del tenant FabricPool.

   c. Se si desidera che questo criterio di traffico limiti il traffico per gli altri endpoint, selezionare **corrispondenza inversa**.

5. Facoltativamente, aggiungere uno o più limiti per controllare il traffico di rete corrispondente alla regola.

   > StorageGRID raccoglie le metriche anche se non si aggiungono limiti, in modo da poter comprendere le tendenze del traffico.

   a. Selezionare **Aggiungi un limite**.

   b. Selezionare il tipo di traffico che si desidera limitare e il limite da applicare.

6. Selezionare **continua**.

7. Leggere e rivedere la policy di classificazione del traffico. Utilizzare il pulsante **precedente** per tornare indietro e apportare le modifiche necessarie. Quando si è soddisfatti della policy, selezionare **Salva e continua**.

Dopo il completamento

"Visualizzare le metriche del traffico di rete" per verificare che i criteri stiano applicando i limiti di traffico previsti.

Informazioni sul copyright

Copyright © 2025 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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.