



# **Configurare FabricPool**

## **StorageGRID**

NetApp  
April 10, 2024

# Sommario

- Configurare FabricPool ..... 1
  - Configure StorageGRID for FabricPool: Panoramica ..... 1
  - Collega StorageGRID come Tier cloud ..... 3
  - Utilizza la gestione del ciclo di vita delle informazioni di StorageGRID con i dati FabricPool ..... 14
  - Creare una policy di classificazione del traffico per FabricPool ..... 17
  - Altre Best practice per StorageGRID e FabricPool ..... 20

# Configurare FabricPool

## Configure StorageGRID for FabricPool: Panoramica

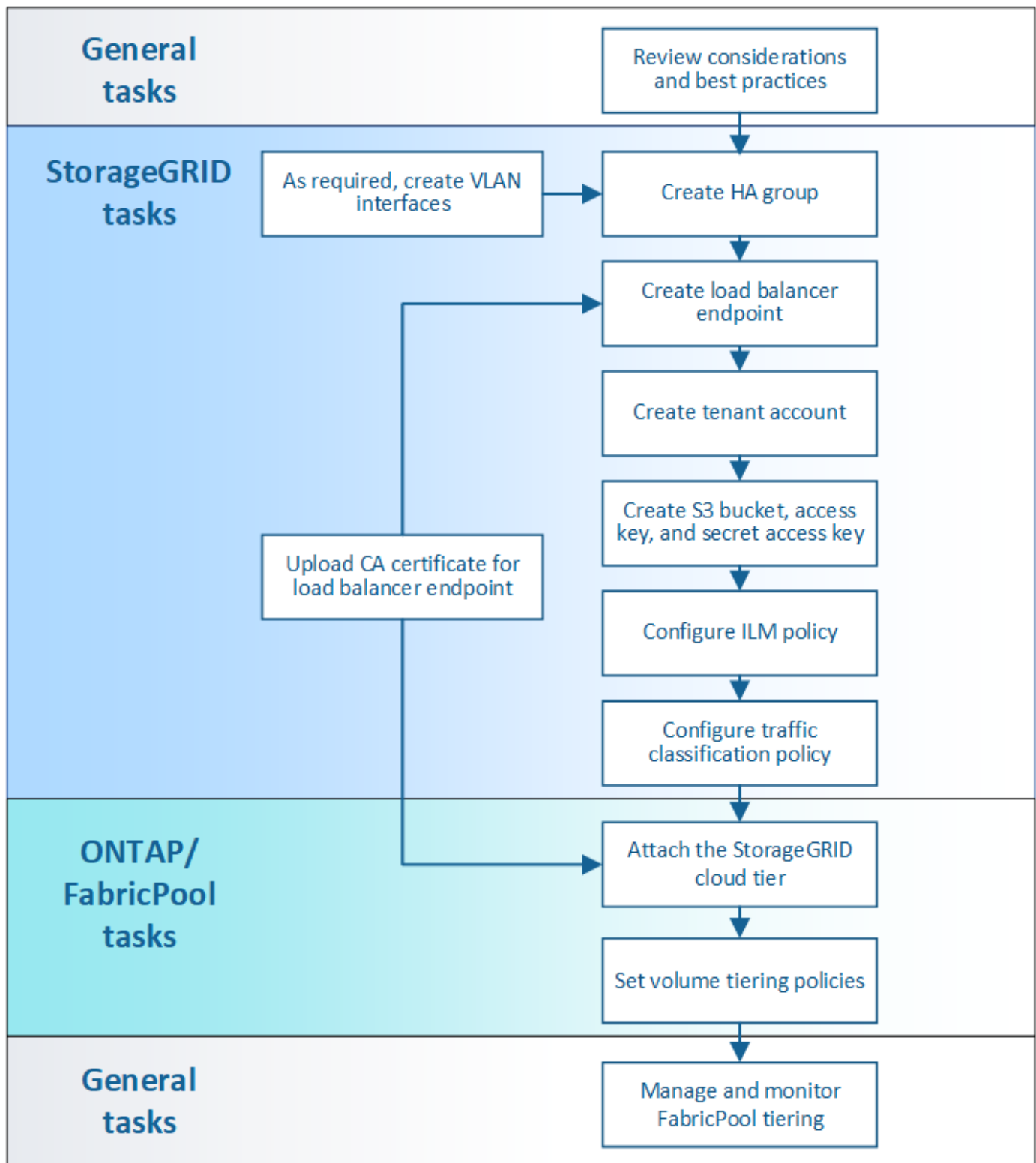
Se si utilizza il software NetApp ONTAP, è possibile utilizzare NetApp FabricPool per eseguire il tiering dei dati inattivi o a freddo su un sistema di storage a oggetti NetApp StorageGRID.

### A proposito di queste istruzioni

Seguire queste istruzioni per:

- Ottieni una panoramica sulla configurazione di un sistema di storage a oggetti StorageGRID per l'utilizzo con FabricPool.
- Scopri come ottenere le informazioni che fornisci a ONTAP quando Aggiungi StorageGRID come Tier cloud FabricPool.
- Scopri le Best practice per la configurazione del criterio ILM (Information Lifecycle Management) di StorageGRID, di un criterio di classificazione del traffico StorageGRID e di altre opzioni StorageGRID per un carico di lavoro FabricPool.

### Workflow di configurazione



## Prima di iniziare

- Decidere quale criterio di tiering dei volumi FabricPool utilizzare per eseguire il tiering dei dati ONTAP inattivi in StorageGRID.
- Pianificare e installare un sistema StorageGRID per soddisfare le esigenze di capacità e performance dello storage.
- Familiarizzare con il software di sistema StorageGRID, incluso il gestore del grid e il gestore del tenant.

- Consulta queste risorse aggiuntive, che forniscono dettagli sull'utilizzo e la configurazione di FabricPool:
  - ["TR-4598: Best practice FabricPool in ONTAP 9.9.1"](#)
  - ["Documentazione di ONTAP 9"](#)

## Che cos'è FabricPool?

FabricPool è una soluzione di storage ibrido ONTAP che utilizza un aggregato flash dalle performance elevate come Tier delle performance e un archivio di oggetti come Tier del cloud. I dati vengono memorizzati sul supporto di storage primario o nel datastore degli oggetti in base al fatto che l'accesso sia frequente o meno. L'utilizzo di aggregati abilitati per FabricPool consente di ridurre i costi dello storage senza compromettere performance, efficienza o protezione.

Non sono necessarie modifiche architetturali e puoi continuare a gestire i dati e l'ambiente applicativo dal sistema di storage centrale ONTAP.

## Che cos'è StorageGRID?

StorageGRID è un'architettura di storage che gestisce i dati come oggetti, rispetto ad altre architetture di storage come lo storage a blocchi o file. Gli oggetti vengono conservati all'interno di un singolo contenitore (ad esempio un bucket) e non vengono nidificati come file all'interno di una directory all'interno di altre directory. Sebbene lo storage a oggetti offra generalmente performance inferiori rispetto allo storage a blocchi o a file, è notevolmente più scalabile. I bucket StorageGRID possono contenere petabyte di dati e miliardi di oggetti.

## Perché utilizzare StorageGRID come Tier cloud FabricPool?

FabricPool può eseguire il tiering dei dati ONTAP a diversi provider di archivi di oggetti, tra cui StorageGRID. A differenza dei cloud pubblici che potrebbero impostare un numero massimo di IOPS (Input/Output Operations per Second) supportati a livello di bucket o container, le performance di StorageGRID sono scalabili in base al numero di nodi in un sistema. L'utilizzo di StorageGRID come livello cloud FabricPool ti consente di conservare i tuoi dati nel tuo cloud privato per ottenere le massime performance e il controllo completo sui tuoi dati.

Inoltre, non è necessaria una licenza FabricPool quando si utilizza StorageGRID come livello cloud.

## È possibile utilizzare più cluster ONTAP con StorageGRID?

Queste istruzioni descrivono come connettere StorageGRID a un singolo cluster ONTAP. Tuttavia, è possibile collegare lo stesso sistema StorageGRID a più cluster ONTAP.

L'unico requisito per il tiering dei dati da più cluster ONTAP a un singolo sistema StorageGRID è l'utilizzo di un bucket S3 diverso per ciascun cluster. In base ai tuoi requisiti, puoi utilizzare lo stesso gruppo ad alta disponibilità (ha), endpoint di bilanciamento del carico e account tenant per tutti i cluster, oppure puoi configurare ciascuno di questi elementi per ciascun cluster.

## Collega StorageGRID come Tier cloud

### Informazioni necessarie per collegare StorageGRID come Tier cloud

Prima di poter collegare StorageGRID come livello cloud per FabricPool, è necessario eseguire alcune fasi di configurazione in StorageGRID e ottenere determinati valori.

**A proposito di questa attività**

La seguente tabella elenca le informazioni da fornire a ONTAP quando si collega StorageGRID come livello cloud per FabricPool. Gli argomenti di questa sezione spiegano come utilizzare il Gestore griglia e il Gestore tenant di StorageGRID per ottenere le informazioni necessarie.



I nomi esatti dei campi elencati e il processo utilizzato per inserire i valori richiesti in ONTAP dipendono dall'utilizzo dell'interfaccia CLI (creazione configurazione archivio oggetti aggregato di storage) o del gestore di sistema ONTAP (**Storage > aggregati e dischi > livello cloud**) di ONTAP.

Per ulteriori informazioni, fare riferimento a quanto segue:

- ["TR-4598: Best practice FabricPool in ONTAP 9.9.1"](#)
- ["Documentazione di ONTAP 9"](#)

Aeroporto ONTAP Field	Descrizione
Nome archivio oggetti	Qualsiasi nome univoco e descrittivo. Ad esempio, StorageGRID_Cloud_Tier.
Tipo di provider	StorageGRID (Gestore di sistema ONTAP) o. SGWS (CLI ONTAP).
Porta	La porta utilizzata da FabricPool per la connessione a StorageGRID. È possibile determinare il numero di porta da utilizzare quando si definisce l'endpoint del bilanciamento del carico di StorageGRID.  <a href="#">Creare un endpoint di bilanciamento del carico per FabricPool</a>
Nome del server	Nome di dominio completo (FQDN) per l'endpoint del bilanciamento del carico di StorageGRID. Ad esempio, s3.storagegrid.company.com.  Tenere presente quanto segue: <ul style="list-style-type: none"><li>• Il nome di dominio specificato deve corrispondere al nome di dominio sul certificato CA caricato per l'endpoint del bilanciamento del carico di StorageGRID.</li><li>• Il record DNS per questo nome di dominio deve essere associato a ciascun indirizzo IP utilizzato per la connessione a StorageGRID.</li></ul> <a href="#">Configurare il server DNS per gli indirizzi IP StorageGRID</a>

Aeroporto ONTAP Field	Descrizione
Nome del container	<p>Il nome del bucket StorageGRID che verrà utilizzato con questo cluster ONTAP. Ad esempio, <code>fabricpool-bucket</code>. È possibile creare questo bucket in Gestione tenant oppure, a partire da Gestione sistema di ONTAP 9.10, è possibile creare il bucket con l'installazione guidata di FabricPool.</p> <p>Tenere presente quanto segue:</p> <ul style="list-style-type: none"> <li>• Una volta creata la configurazione, non è possibile modificare il nome del bucket.</li> <li>• Il bucket non può avere la versione attivata.</li> <li>• È necessario utilizzare un bucket diverso per ogni cluster ONTAP che eseguirà il Tier dei dati in StorageGRID.</li> </ul> <p><a href="#">Creare un bucket S3 e ottenere una chiave di accesso</a></p>
Chiave di accesso e password segreta	<p>La chiave di accesso e la chiave di accesso segreta per l'account tenant StorageGRID.</p> <p>Questi valori vengono generati in Tenant Manager.</p> <p><a href="#">Creare un bucket S3 e ottenere una chiave di accesso</a></p>
SSL	Deve essere attivato.
Certificato dell'archivio di oggetti	<p>Il certificato CA caricato al momento della creazione dell'endpoint del bilanciamento del carico di StorageGRID.</p> <p><b>Nota:</b> se una CA intermedia ha emesso il certificato StorageGRID, è necessario fornire il certificato CA intermedio. Se il certificato StorageGRID è stato emesso direttamente dalla CA principale, è necessario fornire il certificato della CA principale.</p> <p><a href="#">Creare un endpoint di bilanciamento del carico per FabricPool</a></p>

### Al termine

Dopo aver ottenuto le informazioni StorageGRID richieste, puoi accedere a ONTAP per aggiungere StorageGRID come livello cloud, aggiungere il livello cloud come aggregato e impostare le policy di tiering dei volumi.

## Best practice per il bilanciamento del carico

Prima di collegare StorageGRID come livello cloud FabricPool, è necessario utilizzare il gestore di griglia StorageGRID per configurare almeno un endpoint di bilanciamento del carico.

## Cos'è il bilanciamento del carico?

Quando i dati vengono suddivisi in livelli da FabricPool a un sistema StorageGRID, StorageGRID utilizza un sistema di bilanciamento del carico per gestire il carico di lavoro di acquisizione e recupero. Il bilanciamento del carico massimizza la velocità e la capacità di connessione distribuendo il carico di lavoro FabricPool su più nodi di storage.

Il servizio bilanciamento del carico StorageGRID viene installato su tutti i nodi di amministrazione e su tutti i nodi gateway e fornisce il bilanciamento del carico di livello 7. Esegue la terminazione TLS (Transport Layer Security) delle richieste client, ispeziona le richieste e stabilisce nuove connessioni sicure ai nodi di storage.

Il servizio Load Balancer su ciascun nodo funziona in modo indipendente quando si inoltra il traffico client ai nodi di storage. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai nodi di storage con una maggiore disponibilità della CPU.

Anche se il servizio bilanciamento del carico di StorageGRID è il meccanismo di bilanciamento del carico consigliato, potrebbe essere necessario integrare un bilanciamento del carico di terze parti. Per informazioni, contattare il rappresentante commerciale NetApp o visitare il sito Web all'indirizzo ["TR-4626: Bilanciatori di carico globali e di terze parti StorageGRID"](#).



Il servizio separato di bilanciamento del carico di connessione (CLB) sui nodi gateway è obsoleto e non è più consigliato per l'utilizzo con FabricPool.

## Best practice per il bilanciamento del carico StorageGRID

Come Best practice generale, ogni sito del sistema StorageGRID deve includere due o più nodi nel servizio bilanciamento del carico. Ad esempio, un sito potrebbe includere due nodi gateway o sia un nodo amministratore che un nodo gateway. Assicurarsi che vi sia un'infrastruttura di rete, hardware o virtualizzazione adeguata per ciascun nodo di bilanciamento del carico, sia che si utilizzino appliance di servizi SG100 o SG1000, nodi bare metal o nodi basati su macchine virtuali (VM).

È necessario configurare un endpoint del bilanciamento del carico StorageGRID per definire la porta che i nodi gateway e i nodi di amministrazione utilizzeranno per le richieste FabricPool in entrata e in uscita.

## Best practice per il certificato endpoint del bilanciamento del carico

Quando si crea un endpoint di bilanciamento del carico da utilizzare con FabricPool, è necessario utilizzare HTTPS come protocollo. La comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

È quindi possibile caricare un certificato firmato da un'autorità di certificazione pubblica o privata oppure generare un certificato autofirmato. Il certificato consente a ONTAP di autenticarsi con StorageGRID.

Come procedura consigliata, è necessario utilizzare un certificato del server CA per proteggere la connessione. I certificati firmati da una CA possono essere ruotati senza interruzioni.

Quando si richiede un certificato CA per l'utilizzo con l'endpoint del bilanciamento del carico, assicurarsi che il nome di dominio sul certificato corrisponda al nome del server immesso in ONTAP per l'endpoint del bilanciamento del carico. Se possibile, utilizzare un carattere jolly (\*) per consentire gli URL di tipo host virtuale. Ad esempio:

```
*.s3.storagegrid.company.com
```



Quando si aggiunge StorageGRID come livello cloud FabricPool, è necessario installare lo stesso certificato nel cluster ONTAP, nonché i certificati di autorità di certificazione (CA) root e subordinate.



StorageGRID utilizza i certificati del server per diversi scopi. Se ci si connette al servizio Load Balancer, è possibile utilizzare facoltativamente il certificato S3 e Swift API.

Per ulteriori informazioni sul certificato server per un endpoint di bilanciamento del carico:

- [Configurare gli endpoint del bilanciamento del carico](#)
- [Linee guida per la protezione avanzata dei certificati server](#)

## Best practice per i gruppi ad alta disponibilità

Prima di collegare StorageGRID come livello cloud FabricPool, è necessario utilizzare Gestione griglia StorageGRID per configurare un gruppo ad alta disponibilità (ha).

### Che cos'è un gruppo ad alta disponibilità (ha)?

Per garantire che il servizio bilanciamento del carico sia sempre disponibile per gestire i dati FabricPool, è possibile raggruppare le interfacce di rete di più nodi di amministrazione e gateway in una singola entità, nota come gruppo ad alta disponibilità (ha). Se il nodo attivo nel gruppo ha non riesce, un altro nodo del gruppo può continuare a gestire il carico di lavoro.

Ogni gruppo ha fornisce un accesso altamente disponibile ai servizi condivisi sui nodi associati. Ad esempio, un gruppo ha costituito da interfacce solo su nodi gateway o su entrambi i nodi Admin e Gateway fornisce un accesso altamente disponibile al servizio Load Balancer condiviso.

Per creare un gruppo ha, attenersi alla seguente procedura generale:

1. Selezionare le interfacce di rete per uno o più nodi di amministrazione o nodi gateway. È possibile selezionare l'interfaccia Grid Network (eth0), l'interfaccia Client Network (eth2) o un'interfaccia VLAN.



Se si prevede di utilizzare un'interfaccia VLAN per separare il traffico FabricPool, un amministratore di rete deve prima configurare un'interfaccia di trunk e la VLAN corrispondente. Ogni VLAN è identificata da un ID numerico o da un tag. Ad esempio, la rete potrebbe utilizzare la VLAN 100 per il traffico FabricPool.

2. Assegnare uno o più indirizzi IP virtuali (VIP) al gruppo. Le applicazioni client, come FabricPool, possono utilizzare uno qualsiasi di questi indirizzi VIP per connettersi a StorageGRID.
3. Specificare un'interfaccia come principale e determinare l'ordine di priorità per le interfacce di backup. 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 primaria non funziona, gli indirizzi VIP passano alla 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. Questo processo di failover richiede in genere solo pochi secondi ed è abbastanza rapido da consentire alle applicazioni client di avere un impatto minimo e può fare affidamento sui normali comportamenti di ripetizione per continuare a funzionare.

Quando il guasto viene risolto e un'interfaccia con priorità più alta diventa nuovamente disponibile, gli indirizzi VIP vengono automaticamente spostati nell'interfaccia con priorità più alta disponibile.

## Best practice per i gruppi ad alta disponibilità (ha)

Le Best practice per la creazione di un gruppo StorageGRID ha per FabricPool dipendono dal carico di lavoro, come segue:

- Se si prevede di utilizzare FabricPool con i dati del carico di lavoro primario, è necessario creare un gruppo ha che includa almeno due nodi di bilanciamento del carico per evitare l'interruzione del recupero dei dati.
- Se si prevede di utilizzare la policy di tiering del volume solo snapshot di FabricPool o Tier di performance locali non primari (ad esempio, ubicazioni per il disaster recovery o destinazioni NetApp SnapMirror®), è possibile configurare un gruppo ha con un solo nodo.

Queste istruzioni descrivono la configurazione di un gruppo ha per Active-Backup ha (un nodo è attivo e un nodo è il backup). Tuttavia, potrebbe essere preferibile utilizzare DNS Round Robin o Active-Active ha. Per ulteriori informazioni sui vantaggi di queste altre configurazioni ha, vedere [Opzioni di configurazione per i gruppi ha](#).

## Configurare il server DNS per gli indirizzi IP StorageGRID

Dopo aver configurato i gruppi ad alta disponibilità e gli endpoint del bilanciamento del carico, è necessario assicurarsi che il DNS (Domain Name System) del sistema ONTAP includa un record per associare il nome del server StorageGRID (Fully Qualified Domain Name) all'indirizzo IP che FabricPool utilizzerà per stabilire 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, FabricPool si conatterà agli indirizzi IP virtuali di tale gruppo ha.
- Se non si utilizza un gruppo ha, FabricPool può connettersi 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.

## 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 costituito da una o più interfacce di rete su nodi di amministrazione, nodi gateway o entrambi.

### Di cosa hai bisogno

- 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](#).

### A proposito di questa attività

Ogni gruppo ha utilizza indirizzi IP virtuali (VIP) per fornire un accesso altamente disponibile ai servizi condivisi sui nodi associati.

Per ulteriori informazioni su questa attività, vedere [Gestire i gruppi ad alta disponibilità](#).

## Fasi

1. Selezionare **CONFIGURATION > Network > High Availability groups**.
2. Selezionare **Crea**.
3. Immettere un nome univoco e, facoltativamente, una descrizione.
4. Selezionare una o più interfacce da aggiungere a questo gruppo ha.

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

5. Determinare l'interfaccia primaria e le interfacce di backup per questo gruppo ha.

Trascinare e rilasciare 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 VIP si spostano sulla 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. Specificare la 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.

7. Se si desidera, 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.
8. Inserire uno o più indirizzi IP virtuali per il gruppo ha. È possibile aggiungere fino a 10 indirizzi IP. Tutti i VIP devono trovarsi all'interno della subnet VIP.

Specificare almeno un indirizzo IPv4. In alternativa, è possibile specificare ulteriori indirizzi IPv4 e IPv6.

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

## Creare un endpoint di bilanciamento del carico per FabricPool

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

### Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un [browser web supportato](#).
- Si dispone dell'autorizzazione di accesso root.
- Sono disponibili i seguenti file:
  - Server Certificate (certificato server): Il file di certificato del server personalizzato.
  - Server Certificate Private Key (chiave privata certificato server): Il file di chiave privata del certificato del server personalizzato.

- **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.

### A proposito di questa attività

Per ulteriori informazioni su questa attività, vedere [Configurare gli endpoint del bilanciamento del carico](#).

### Fasi

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

**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

3. Inserire i dettagli dell'endpoint.

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint

Campo	Descrizione
Porta	<p>La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è 10433, ma è possibile inserire qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway, poiché queste porte sono riservate sui nodi Admin.</p> <p><b>Nota:</b> le porte utilizzate da altri servizi di rete non sono consentite. Vedere <a href="#">Riferimento porta di rete</a>.</p> <p>Quando si collega StorageGRID come livello cloud FabricPool, è necessario fornire lo stesso numero di porta a ONTAP.</p>
Tipo di client	Selezionare <b>S3</b> .
Protocollo di rete	<p>Selezionare <b>HTTPS</b>.</p> <p><b>Nota:</b> L'utilizzo di <b>HTTP</b> è supportato ma non consigliato.</p>

4. Selezionare **continua**.

5. Specificare la modalità di binding.

Utilizzare l'impostazione **Global** (scelta consigliata) o limitare l'accessibilità di questo endpoint a una delle seguenti opzioni:

- Interfacce di rete specifiche di nodi specifici.
- Indirizzi IP virtuali (VIP) specifici ad alta disponibilità (ha). Utilizzare questa opzione solo se si richiedono livelli di isolamento dei carichi di lavoro molto più elevati.

6. Selezionare **continua**.

7. Selezionare **carica certificato** (consigliato), quindi selezionare il certificato del server, la chiave privata del certificato e il bundle CA opzionale.

8. 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.

### Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un [browser web supportato](#).
- Si dispone di autorizzazioni di accesso specifiche.

### A proposito di questa attività

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.

È possibile utilizzare lo stesso account tenant per più cluster ONTAP. In alternativa, è possibile creare un account tenant dedicato per ciascun cluster ONTAP, in base alle esigenze.



Queste istruzioni presuppongono che sia stato configurato il Single Sign-on (SSO) per Grid Manager. Se SSO non è attivato, utilizzare [queste istruzioni per creare un account tenant](#) invece.

## Fasi

1. Selezionare **TENANT**.
2. Selezionare **Crea**.
3. Inserire un nome visualizzato e una descrizione.
4. Selezionare **S3**.
5. Lasciare vuoto il campo **quota di storage**.
6. Selezionare **Allow platform Services** (Consenti servizi piattaforma) per abilitare l'utilizzo dei servizi della piattaforma.

Se i servizi della piattaforma sono attivati, un tenant può utilizzare funzionalità, come la replica CloudMirror, che accedono ai servizi esterni.

7. Non selezionare **Usa origine identità propria**.
8. Non selezionare **Allow S3 Select** (Consenti selezione S3).
9. Selezionare un gruppo federated esistente da Grid Manager per disporre dell'autorizzazione di accesso root iniziale per il tenant.
10. Selezionare **Crea tenant**.

## Creare un bucket S3 e ottenere una chiave 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.

### Di cosa hai bisogno

- È stato creato un account tenant per l'utilizzo di FabricPool.

### A proposito di questa attività

Queste istruzioni descrivono come utilizzare il gestore tenant StorageGRID per creare un bucket e ottenere le chiavi di accesso. È inoltre possibile eseguire queste attività utilizzando l'API di gestione dei tenant o l'API REST di StorageGRID S3. In alternativa, se si utilizza ONTAP 9.10, è possibile creare il bucket utilizzando l'installazione guidata di FabricPool.

Per saperne di più:

- [Utilizzare un account tenant](#)
- [Utilizzare S3](#)

## 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.

- Selezionare **STORAGE (S3) > Bucket**.
- Selezionare **Crea bucket**.
- Immettere il nome del bucket StorageGRID che si intende utilizzare con FabricPool. Ad esempio, `fabricpool-bucket`.



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

I nomi dei bucket devono essere conformi alle seguenti regole:

- Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant).
- Deve essere conforme al DNS.
- Deve contenere almeno 3 e non più di 63 caratteri.
- Può essere una serie di una o più etichette, con etichette adiacenti separate da un punto. Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini.
- Non deve essere simile a un indirizzo IP formattato con testo.
- Non utilizzare i periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server.

- Selezionare la regione per questo bucket.

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

## Create bucket



### Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name

fabricpool-bucket

Region

us-east-1

Cancel

Create bucket

e. Selezionare **Crea bucket**.



Per i bucket FabricPool, il livello di coerenza consigliato è **Read-after-new-write**, che è l'impostazione predefinita per un nuovo bucket. Non modificare i bucket FabricPool per utilizzare **Available** o qualsiasi altro livello di coerenza.

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

- Selezionare **STORAGE (S3) > My access key**.
- Selezionare **Crea chiave**.
- Selezionare **Crea chiave di accesso**.
- 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 creano una nuova chiave di accesso e una chiave di accesso segreta, ricordarsi di aggiornare immediatamente i valori corrispondenti in ONTAP per garantire che ONTAP possa memorizzare e recuperare i dati in StorageGRID senza interruzioni.

## Utilizza la gestione del ciclo di vita delle informazioni di StorageGRID con i dati FabricPool

Se si utilizza FabricPool per eseguire il tiering dei dati in StorageGRID, è necessario comprendere i requisiti per la creazione di regole ILM (Information Lifecycle Management) di StorageGRID e una policy ILM per la gestione dei dati FabricPool. È



necessario garantire che le regole ILM applicabili ai dati FabricPool non siano disgreganti.



FabricPool non conosce le regole o le policy ILM di StorageGRID. La perdita di dati può verificarsi se il criterio ILM di StorageGRID non è configurato correttamente. Vedere [Gestire gli oggetti con ILM](#) Per istruzioni ILM dettagliate.

Consulta queste linee guida per assicurarti che le tue regole ILM e le policy ILM siano adatte ai dati FabricPool e ai tuoi requisiti di business. Se si utilizza già ILM di StorageGRID, potrebbe essere necessario aggiornare il criterio ILM attivo per soddisfare queste linee guida.

- Puoi utilizzare qualsiasi combinazione di regole di replica e erasure coding per proteggere i dati del livello cloud.

La Best practice consigliata consiste nell'utilizzare la codifica di cancellazione 2+1 all'interno di un sito per una protezione dei dati conveniente. L'erasure coding utilizza più CPU, ma offre una capacità di storage significativamente inferiore rispetto alla replica. Gli schemi 4+1 e 6+1 utilizzano una capacità inferiore rispetto allo schema 2+1. Tuttavia, gli schemi 4+1 e 6+1 sono meno flessibili se è necessario aggiungere nodi di storage durante l'espansione della griglia. Per ulteriori informazioni, vedere [Aggiungere capacità di storage per gli oggetti con codifica per la cancellazione](#).

- Ogni regola applicata ai dati FabricPool deve utilizzare la codifica di cancellazione oppure creare almeno due copie replicate.



Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

- Non utilizzare una regola ILM che scadrà o eliminerà i dati del livello cloud di FabricPool. Impostare il periodo di conservazione in ogni regola ILM su "Perforever" per garantire che gli oggetti FabricPool non vengano eliminati da ILM StorageGRID.
- Non creare regole che spostino i dati del Tier cloud FabricPool dal bucket a un'altra posizione. Non è possibile utilizzare le regole ILM per archiviare i dati FabricPool su nastro utilizzando un nodo di archiviazione o utilizzare un pool di storage cloud per spostare i dati FabricPool in un altro archivio di oggetti.



L'utilizzo dei pool di storage cloud con FabricPool non è supportato a causa della latenza aggiunta per recuperare un oggetto dalla destinazione del pool di storage cloud.

- A partire da ONTAP 9.8, è possibile creare tag a oggetti per semplificare la classificazione e l'ordinamento dei dati a più livelli. Ad esempio, è possibile impostare i tag solo sui volumi FabricPool collegati a StorageGRID. Quindi, quando si creano le regole ILM in StorageGRID, è possibile utilizzare il filtro avanzato tag oggetto per selezionare e inserire questi dati.

## Esempio di policy ILM per i dati FabricPool

Utilizza 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](#).

## Fasi

1. Creare un pool di storage denominato **DEN**. Selezionare il sito di Denver.
2. Creare un profilo di codifica Erasure denominato **2 più 1**. Selezionare lo schema di erasure coding 2+1 e il pool di storage **DEN**.
3. 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 regola	2 più 1 erasure coding per i dati FabricPool
Nome bucket	<code>fabricpool-bucket</code>  È anche possibile filtrare l'account tenant FabricPool.
Filtraggio avanzato	Dimensione oggetto (MB) maggiore di 0.2 MB.  <b>Nota:</b> FabricPool scrive solo oggetti da 4 MB, ma è necessario aggiungere un filtro dimensione oggetto perché questa regola utilizza la codifica di cancellazione.
Tempo di riferimento	Tempo di acquisizione
Posizionamento	Dal giorno 0 memorizzare per sempre
Tipo	Codifica di cancellazione
Posizione	DEN (2 più 1)
Comportamento di acquisizione	Bilanciato

4. Creare una regola ILM che creerà 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 regola	Due copie replicate
Nome bucket	<i>nessuno</i>

Definizione della regola	Valore di esempio
Filtraggio avanzato	<i>nessuno</i>
Tempo di riferimento	Tempo di acquisizione
Posizionamento	Dal giorno 0 memorizzare per sempre
Tipo	Replicato
Posizione	DEN
Copie	2
Comportamento di acquisizione	Bilanciato

5. 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.
6. Acquisire oggetti di test nella griglia.
7. Simulare il criterio con gli oggetti di test per verificare il comportamento.
8. 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 replicate e codificate in cancellazione verranno conservate in StorageGRID fino a quando non verranno eliminate dal client S3. StorageGRID ILM non eliminerà mai questi elementi.

## 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.

### Di cosa hai bisogno

- 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.

- Come regola generale, 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.

Per saperne di più: [Gestire le policy di classificazione del traffico](#)

### Fasi

1. Selezionare **CONFIGURAZIONE > rete > classificazione del traffico**.
2. Inserire un nome e una descrizione.
3. Nella sezione regole corrispondenti, creare almeno una regola.
  - a. Selezionare **Crea**.
  - b. Selezionare **endpoint** 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**.
4. Facoltativamente, creare uno o più limiti.



Anche se non sono stati impostati limiti per una policy di classificazione del traffico, vengono raccolte metriche in modo da poter comprendere le tendenze del traffico.

- a. Selezionare **Crea**.
- b. Selezionare il tipo di traffico che si desidera limitare e il limite da applicare.

Questo esempio di criterio di classificazione del traffico FabricPool mostra i tipi di traffico di rete che è possibile limitare e i tipi di valori che è possibile selezionare. I limiti di una policy effettiva si baserebbero sui requisiti specifici dell'utente.

## Policy

Name 

FabricPool

Description (optional)

Limit traffic other than FabricPool

## Matching Rules

Traffic that matches any rule is included in the policy.

 Create

 Edit

 Remove

Type	Inverse Match	Match Value
<input checked="" type="radio"/> Endpoint		FabricPool (https 10443)

Displaying 1 matching rule.

## Limits (Optional)

 Create

 Edit

 Remove

Type	Value	Units
<input type="radio"/> Concurrent Read Requests	50	Concurrent Requests
<input type="radio"/> Concurrent Read Requests	15	Concurrent Requests
<input type="radio"/> Read Request Rate	100	Requests/Second
<input type="radio"/> Write Request Rate	25	Requests/Second
<input type="radio"/> Per-Request Bandwidth In	2000000	Bytes/Second
<input checked="" type="radio"/> Per-Request Bandwidth Out	10000000	Bytes/Second

5. Dopo aver creato il criterio di classificazione del traffico, selezionare il criterio, quindi selezionare **metriche** per determinare se il criterio limita il traffico come previsto.

## Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

<div><span>+ Create</span> <span>Edit</span> <span>Remove</span> <span>Metrics</span></div>		
Name	Description	ID
<input checked="" type="radio"/> FabricPool	Limit traffic other than FabricPool	587f53b2-7cf2-44b9-af5c-694ebbd4a2c5
Displaying 1 traffic classification policy.		

## Altre Best practice per StorageGRID e FabricPool

Quando si configura un sistema StorageGRID per l'utilizzo con FabricPool, evitare di impostare opzioni globali che potrebbero influire sul modo in cui i dati vengono salvati.

### Crittografia degli oggetti

Durante la configurazione di StorageGRID, è possibile attivare l'impostazione globale **crittografia oggetto memorizzato** se è richiesta la crittografia dei dati per altri client StorageGRID (**CONFIGURAZIONE > sistema > Opzioni griglia**). I dati a più livelli da FabricPool a StorageGRID sono già crittografati, pertanto l'attivazione dell'impostazione StorageGRID non è necessaria. Le chiavi di crittografia lato client sono di proprietà di ONTAP.

### Compressione degli oggetti

Durante la configurazione di StorageGRID, non attivare l'impostazione globale **compress stored objects** (**CONFIGURATION > System > Grid options**). I dati a più livelli da FabricPool a StorageGRID sono già compressi. L'attivazione di **compress stored objects** non riduce ulteriormente la dimensione di un oggetto.

### Livello di coerenza

Per i bucket FabricPool, il livello di coerenza consigliato è **Read-after-new-write**, che è l'impostazione predefinita per un nuovo bucket. Non modificare i bucket FabricPool per utilizzare **Available** o qualsiasi altro livello di coerenza.

### Tiering FabricPool

Se il nodo StorageGRID utilizza lo storage assegnato da un sistema NetApp ONTAP, verificare che il volume non disponga di un criterio di tiering FabricPool attivato. Ad esempio, se un nodo StorageGRID è in esecuzione su un host VMware, assicurarsi che il volume che esegue il backup del datastore per il nodo StorageGRID non abbia un criterio di tiering FabricPool attivato. La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.



Non utilizzare mai FabricPool per eseguire il tiering dei dati relativi a StorageGRID su StorageGRID. Il tiering dei dati StorageGRID su StorageGRID aumenta la risoluzione dei problemi e la complessità operativa.

## 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.