



Best practice di StorageGRID per FabricPool

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from <https://docs.netapp.com/it-it/storagegrid-120/fabricpool/best-practices-for-high-availability-groups.html> on July 23, 2026. Always check docs.netapp.com for the latest.

Sommario

- Best practice di StorageGRID per FabricPool 1
 - Best practice per i gruppi HA (alta disponibilità) di StorageGRID con FabricPool 1
 - Che cos'è un gruppo HA? 1
 - Utilizzo dei gruppi HA 1
 - Best practice per il bilanciamento del carico di StorageGRID con FabricPool 1
 - Best practice per l'accesso del tenant all'endpoint del bilanciamento del carico utilizzato per FabricPool 1
 - Best practice per il certificato di sicurezza 2
- Procedure consigliate per l'utilizzo di StorageGRID ILM con i dati FabricPool 3
 - Linee guida per l'utilizzo di ILM con FabricPool 3
- Best practice per le impostazioni globali di StorageGRID con FabricPool 4
 - Segmenti 4
 - Segmenti 4
 - compressione degli oggetti 4
 - Blocco oggetto S3 4
 - coerenza del bucket 4
 - tiering FabricPool 5

Best practice di StorageGRID per FabricPool

Best practice per i gruppi HA (alta disponibilità) di StorageGRID con FabricPool

Prima di collegare StorageGRID come livello cloud FabricPool, informati sui gruppi di alta disponibilità (HA) di StorageGRID e rivedi le best practice per l'utilizzo dei gruppi HA con FabricPool.

Che cos'è un gruppo HA?

Un gruppo ad alta disponibilità (HA) è una raccolta di interfacce provenienti da più nodi gateway di StorageGRID, nodi di amministrazione o entrambi. Un gruppo HA aiuta a mantenere disponibili le connessioni dati dei client. 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 di FabricPool.

Ogni gruppo HA fornisce accesso ad alta disponibilità ai servizi condivisi sui nodi associati. Ad esempio, un gruppo HA composto da interfacce presenti solo sui Gateway Nodes o sia sugli Admin Nodes che sui Gateway Nodes fornisce accesso ad alta disponibilità al servizio di Load Balancer condiviso.

Per saperne di più sui gruppi ad alta disponibilità, vedi ["\\${post_edited_translations.segment}"](#).

Utilizzo dei gruppi HA

Le best practice per creare un gruppo HA di StorageGRID per FabricPool dipendono dal carico di lavoro.

- Se prevedi di utilizzare FabricPool con i dati del carico di lavoro primario, devi creare un gruppo HA che includa almeno due nodi di bilanciamento del carico per evitare interruzioni nel recupero dei dati.
- Se pianifichi di utilizzare la policy di tiering dei volumi snapshot-only di FabricPool o tier di performance locali non primari (ad esempio, sedi di disaster recovery o destinazioni NetApp SnapMirror®), puoi configurare un gruppo HA con un solo nodo.

Queste istruzioni descrivono come configurare un gruppo HA per l'HA Active-Backup (un nodo è attivo e un nodo è di backup). Tuttavia, potresti preferire l'utilizzo di DNS Round Robin o dell'HA Active-Active. Per conoscere i vantaggi di queste altre configurazioni HA, consulta ["Opzioni di configurazione per i gruppi HA"](#).

Best practice per il bilanciamento del carico di StorageGRID con FabricPool

Prima di collegare StorageGRID come tier cloud FabricPool, consulta le best practice per l'utilizzo dei bilanciatori del carico con FabricPool.

Per informazioni generali sul bilanciatore di carico StorageGRID e sul certificato del bilanciatore di carico, vedi ["Considerazioni sul bilanciamento del carico"](#).

Best practice per l'accesso del tenant all'endpoint del bilanciamento del carico utilizzato per FabricPool

Puoi controllare quali tenant possono utilizzare un endpoint del bilanciamento del carico specifico per accedere

ai propri bucket. Puoi consentire tutti i tenant, consentire alcuni tenant o bloccare alcuni tenant. Quando crei un endpoint del bilanciamento del carico per l'uso di FabricPool, seleziona **Consenti tutti i tenant**. ONTAP crittografa i dati inseriti nei bucket StorageGRID, quindi questo livello di sicurezza aggiuntivo fornirebbe una sicurezza supplementare minima.

Best practice per il certificato di sicurezza

Quando crei un endpoint di bilanciamento del carico StorageGRID per l'uso con FabricPool, fornisci il certificato di sicurezza che permetterà a ONTAP di autenticarsi con StorageGRID.

Nella maggior parte dei casi, la connessione tra ONTAP e StorageGRID dovrebbe utilizzare la crittografia Transport Layer Security (TLS). L'utilizzo di FabricPool senza crittografia TLS è supportato ma non consigliato. Quando selezioni il protocollo di rete per l'endpoint del bilanciamento del carico di StorageGRID, seleziona **HTTPS**. Fornisci quindi il certificato di sicurezza che consentirà a ONTAP di autenticarsi con StorageGRID.

`${post_edited_translations.segment}`

- ["Gestisci i certificati di sicurezza"](#)
- ["Considerazioni sul bilanciamento del carico"](#)
- ["\\${post_edited_translations.segment}"](#)

Aggiungi certificato a ONTAP

Quando aggiungi StorageGRID come cloud tier FabricPool, devi installare lo stesso certificato sul cluster ONTAP, inclusi i certificati root e di qualsiasi autorità di certificazione (CA) subordinata.

Gestisci la scadenza dei certificati



Se il certificato utilizzato per proteggere la connessione tra ONTAP e StorageGRID scade, FabricPool smetterà temporaneamente di funzionare e ONTAP perderà temporaneamente l'accesso ai dati sottoposti a tiering su StorageGRID.

`${post_edited_translations.segment}`

- Monitora attentamente tutti gli avvisi che segnalano l'imminente scadenza dei certificati, come gli avvisi **Expiration of load balancer endpoint certificate** e **Expiration of global server certificate for S3 API**.
- Mantieni sempre sincronizzate le versioni StorageGRID e ONTAP del certificato. Se sostituisci o rinnovi il certificato utilizzato per un endpoint del bilanciamento del carico, devi sostituire o rinnovare il certificato equivalente utilizzato da ONTAP per il cloud tier.
- Utilizza un certificato CA firmato pubblicamente. Se utilizzi un certificato firmato da una CA, puoi usare l'API Grid Management per automatizzare la rotazione dei certificati. Questo ti consente di sostituire i certificati in scadenza senza interruzioni.
- Se hai generato un certificato StorageGRID autofirmato e questo sta per scadere, devi sostituire manualmente il certificato sia in StorageGRID che in ONTAP prima che il certificato esistente scada. Se un certificato autofirmato è già scaduto, disattiva la convalida del certificato in ONTAP per evitare la perdita dell'accesso.

Vedi ["NetApp Knowledge Base: Come configurare un nuovo certificato server autofirmato StorageGRID su una distribuzione ONTAP FabricPool esistente"](#) per le istruzioni.

Procedure consigliate per l'utilizzo di StorageGRID ILM con i dati FabricPool

Se utilizzi FabricPool per spostare i dati in tier su StorageGRID, devi comprendere i requisiti per l'utilizzo della gestione del ciclo di vita delle informazioni (ILM) di StorageGRID con i dati FabricPool.



FabricPool non è a conoscenza delle regole o delle policy ILM di StorageGRID. Se la policy ILM di StorageGRID è configurata in modo errato, si può verificare una perdita di dati. Per informazioni dettagliate, consulta "[\\${post_edited_translations.segment}](#)" e "[\\${post_edited_translations.segment}](#)".

Linee guida per l'utilizzo di ILM con FabricPool

Quando usi la FabricPool setup wizard, il wizard crea automaticamente una nuova regola ILM per ogni bucket S3 che crei e aggiunge quella regola a una policy inattiva. Ti viene chiesto di attivare la policy. La regola creata automaticamente segue le best practice consigliate: utilizza la codifica di cancellazione 2+1 in un singolo sito.

Se configuri StorageGRID manualmente invece di usare il FabricPool setup wizard, controlla queste linee guida per assicurarti che le regole e la policy ILM siano adatte ai dati FabricPool e alle tue esigenze aziendali. Potresti dover creare nuove regole e aggiornare le policy ILM attive per rispettare queste linee guida.

- Puoi usare qualsiasi combinazione di regole di replica e di codifica di cancellazione per proteggere i dati del livello cloud.

La best practice consigliata è utilizzare la codifica di cancellazione 2+1 all'interno di un sito per una protezione dei dati conveniente. La codifica di cancellazione utilizza più CPU, ma offre una capacità di archiviazione significativamente inferiore rispetto alla replica. Gli schemi 4+1 e 6+1 utilizzano meno capacità rispetto allo schema 2+1. Tuttavia, gli schemi 4+1 e 6+1 sono meno flessibili se devi aggiungere Storage Nodes durante l'espansione della grid. Per dettagli, vedi "[\\${post_edited_translations.segment}](#)".

- Ogni regola applicata ai dati FabricPool deve utilizzare la codifica di cancellazione oppure deve 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, quell'oggetto viene perso se un nodo di archiviazione ha un guasto o un errore significativo. Perdi anche temporaneamente l'accesso all'oggetto durante le procedure di manutenzione come gli aggiornamenti.

- Se hai bisogno di "[rimuovere i dati FabricPool da StorageGRID](#)", usa ONTAP per recuperare tutti i dati del volume FabricPool e promuoverli al livello di prestazioni.



Per evitare la perdita di dati, non usare una regola ILM che scada o elimini i dati del livello cloud FabricPool. Imposta il periodo di conservazione in ogni regola ILM su **forever** per assicurarti che gli oggetti FabricPool non vengano eliminati da StorageGRID ILM.

- Non creare regole che spostino i dati del livello cloud FabricPool dal bucket in un'altra posizione. Non puoi usare un Cloud Storage Pool per spostare i dati FabricPool in un altro archivio di oggetti.



L'uso di Cloud Storage Pool con FabricPool non è supportato a causa della latenza aggiuntiva per recuperare un oggetto dal target del Cloud Storage Pool.

- A partire da ONTAP 9.8, puoi creare facoltativamente tag per gli oggetti per aiutarti a classificare e ordinare i dati a livelli e gestirli più facilmente. Ad esempio, puoi impostare i tag solo sui volumi FabricPool collegati a StorageGRID. Poi, quando crei regole ILM in StorageGRID, puoi usare il filtro avanzato Object Tag per selezionare e posizionare questi dati.

Best practice per le impostazioni globali di StorageGRID con FabricPool

Quando configuri un sistema StorageGRID per l'utilizzo con FabricPool, potresti dover modificare altre opzioni di StorageGRID. Prima di modificare un'impostazione globale, considera in che modo la modifica influirà sulle altre applicazioni S3.

`$_post_edited_translations.segment`

FabricPool carichi di lavoro spesso presentano un'elevata frequenza di operazioni di lettura, che possono generare un elevato volume di messaggi di audit.

- Se non hai bisogno di un record delle operazioni di lettura dei client per FabricPool o qualsiasi altra applicazione S3, facoltativamente vai su **Configuration > Monitoring > Audit and syslog server**. Modifica l'impostazione **Client Reads in Error** per ridurre il numero di messaggi di audit registrati nel log di audit. Vedi ["Configura la gestione dei log e il server syslog esterno"](#) per i dettagli.
- Se hai una griglia di grandi dimensioni, usi diversi tipi di applicazioni S3 o vuoi conservare tutti i dati di audit, configura un syslog server esterno e salva le informazioni di audit in remoto. Usare un server esterno riduce al minimo l'impatto sulle prestazioni della registrazione dei messaggi di audit senza ridurre la completezza dei dati di audit. Vedi ["\\$\\$_post_edited_translations.segment"](#) per i dettagli.

`$_post_edited_translations.segment`

Quando configuri StorageGRID, puoi opzionalmente abilitare la ["opzione globale per la crittografia degli oggetti memorizzati"](#) se è richiesta la crittografia dei dati per altri client StorageGRID. I dati che vengono trasferiti da FabricPool a StorageGRID sono già crittografati, quindi non è necessario abilitare l'impostazione StorageGRID. Le chiavi di crittografia lato client sono di proprietà di ONTAP.

compressione degli oggetti

Quando configuri StorageGRID, non abilitare ["\\$\\$_post_edited_translations.segment"](#). I dati che vengono spostati da FabricPool a StorageGRID sono già compressi. Usare l'opzione StorageGRID non ridurrà ulteriormente le dimensioni di un oggetto.

Blocco oggetto S3

Se l'impostazione globale S3 Object Lock è abilitata per il tuo sistema StorageGRID, non abilitare ["Blocco oggetto S3"](#) quando crei i bucket FabricPool. S3 Object Lock non è supportato per i bucket FabricPool.

coerenza del bucket

Per i bucket FabricPool, la consistenza consigliata è **Read-after-new-write**, che è la consistenza predefinita

per un nuovo bucket. Non modificare i bucket FabricPool per utilizzare **Available** o **Strong-site**.

tiering FabricPool

Se un nodo StorageGRID utilizza storage assegnato da un sistema NetApp ONTAP, assicurati che il volume non abbia una policy di tiering FabricPool abilitata. Ad esempio, se un nodo StorageGRID è in esecuzione su un host VMware, assicurati che il volume che supporta il datastore per il nodo StorageGRID non abbia una policy di tiering FabricPool abilitata. Disabilitare il 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 trasferire qualsiasi dato relativo a StorageGRID nuovamente su StorageGRID stesso. Il tiering dei dati di StorageGRID nuovamente su StorageGRID aumenta la complessità della risoluzione dei problemi e delle operazioni.

Informazioni sul copyright

Copyright © 2026 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.