



# **StorageGRID Best Practices für FabricPool**

**StorageGRID 11.8**

NetApp  
May 10, 2024

# Inhalt

- StorageGRID Best Practices für FabricPool ..... 1
  - Best Practices für Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen) ..... 1
  - Best Practices für Lastausgleich für FabricPool ..... 1
  - Best Practices für die Verwendung von ILM mit FabricPool-Daten ..... 3
  - Weitere Best Practices für StorageGRID und FabricPool ..... 4

# StorageGRID Best Practices für FabricPool

## Best Practices für Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen)

Bevor Sie StorageGRID als FabricPool-Cloud-Tier hinzufügen, erfahren Sie mehr über StorageGRID HA-Gruppen (High Availability, Hochverfügbarkeit) und lesen Sie die Best Practices zur Verwendung von HA-Gruppen mit FabricPool durch.

### Was ist eine HA-Gruppe?

Eine HA-Gruppe (High Availability, Hochverfügbarkeit) ist eine Sammlung von Schnittstellen aus mehreren StorageGRID Gateway-Nodes, Admin-Nodes oder beidem. Eine HA-Gruppe hilft, Client-Datenverbindungen verfügbar zu halten. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload mit geringer Auswirkung auf die FabricPool-Vorgänge managen.

Jede HA-Gruppe ermöglicht einen hochverfügbaren Zugriff auf die Shared Services auf den zugehörigen Nodes. Beispielsweise bietet eine HA-Gruppe, die aus Schnittstellen nur auf Gateway-Nodes oder sowohl Admin-Nodes als auch Gateway-Nodes besteht, einen hochverfügbaren Zugriff auf den Shared Load Balancer Service.

Weitere Informationen zu Hochverfügbarkeitsgruppen finden Sie unter "[Managen Sie Hochverfügbarkeitsgruppen \(High Availability Groups, HA-Gruppen\)](#)".

### Verwenden von HA-Gruppen

Die Best Practices für die Erstellung einer StorageGRID HA-Gruppe für FabricPool hängen von den Workloads ab.

- Wenn Sie FabricPool für primäre Workload-Daten verwenden möchten, müssen Sie eine HA-Gruppe erstellen, die mindestens zwei Nodes für Lastausgleich enthält, um eine Unterbrechung des Datenabrufs zu verhindern.
- Wenn Sie eine FabricPool Richtlinie für das reine Volume-Tiering nur für Snapshots oder nicht für lokale Performance-Tiers (z. B. Disaster Recovery-Standorte oder NetApp SnapMirror Ziele) verwenden möchten, können Sie eine HA-Gruppe mit nur einem Node konfigurieren.

Diese Anweisungen beschreiben die Einrichtung einer HA-Gruppe für Active-Backup HA (ein Node ist aktiv und ein Node ist ein Backup). Möglicherweise verwenden Sie jedoch lieber DNS Round Robin oder Active-Active HA. Informationen zu den Vorteilen dieser anderen HA-Konfigurationen finden Sie unter "[Konfigurationsoptionen für HA-Gruppen](#)".

## Best Practices für Lastausgleich für FabricPool

Bevor Sie StorageGRID als FabricPool-Cloud-Tier einbinden, sollten Sie sich die Best Practices für die Verwendung von Load Balancern mit FabricPool ansehen.

Allgemeine Informationen zum StorageGRID Load Balancer und zum Load Balancer-Zertifikat finden Sie unter "[Überlegungen zum Lastausgleich](#)".

## Best Practices für den Mandantenzugriff auf den für FabricPool verwendeten Load Balancer-Endpoint

Sie können steuern, welche Mandanten einen bestimmten Load Balancer-Endpoint für den Zugriff auf ihre Buckets verwenden können. Sie können alle Mandanten erlauben, einige Mandanten zulassen oder einige Mandanten blockieren. Wenn Sie einen Endpoint für die Lastverteilung für die FabricPool-Nutzung erstellen, wählen Sie **Alle Mandanten zulassen** aus. ONTAP verschlüsselt die in StorageGRID Buckets gespeicherten Daten, sodass diese zusätzliche Sicherheitsschicht nur wenig zusätzliche Sicherheit bietet.

## Best Practices für das Sicherheitszertifikat

Wenn Sie einen StorageGRID Load Balancer-Endpoint für die Verwendung mit FabricPool erstellen, geben Sie das Sicherheitszertifikat an, mit dem ONTAP sich mit StorageGRID authentifizieren kann.

In den meisten Fällen sollte bei der Verbindung zwischen ONTAP und StorageGRID die TLS-Verschlüsselung (Transport Layer Security) verwendet werden. Die Verwendung von FabricPool ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen. Wenn Sie das Netzwerkprotokoll für den Endpoint des StorageGRID Load Balancer auswählen, wählen Sie **HTTPS** aus. Stellen Sie dann das Sicherheitszertifikat bereit, mit dem ONTAP sich mit StorageGRID authentifizieren kann.

Weitere Informationen zum Serverzertifikat für einen Lastausgleichsendpunkt:

- ["Verwalten von Sicherheitszertifikaten"](#)
- ["Überlegungen zum Lastausgleich"](#)
- ["Härtungsrichtlinien für Serverzertifikate"](#)

## Zertifikat zu ONTAP hinzufügen

Wenn Sie StorageGRID als FabricPool-Cloud-Tier hinzufügen, müssen Sie dasselbe Zertifikat auf dem ONTAP-Cluster installieren, einschließlich des Stammzertifikats und aller untergeordneten Zertifizierungsstellenzertifikate.

## Managen Sie den Ablauf des Zertifikats



Wenn das Zertifikat zur Sicherung der Verbindung zwischen ONTAP und StorageGRID ausläuft, funktioniert FabricPool vorübergehend nicht mehr, und ONTAP verliert vorübergehend den Zugriff auf Daten, die auf StorageGRID-Daten verteilt sind.

Befolgen Sie die folgenden Best Practices, um Probleme mit dem Ablauf von Zertifikaten zu vermeiden:

- Überwachen Sie sorgfältig alle Warnungen, die darauf hinweisen, dass sich das Ablaufdatum des Zertifikats nähert, z. B. das Endpointzertifikat **Ablauf des Load Balancer** und **Ablauf des globalen Serverzertifikats für S3- und Swift-API**-Warnungen.
- Halten Sie die StorageGRID- und ONTAP-Versionen des Zertifikats immer synchron. Wenn Sie das für einen Load Balancer-Endpoint verwendete Zertifikat ersetzen oder erneuern, müssen Sie das von ONTAP für die Cloud-Tier verwendete Zertifikat ersetzen oder erneuern.
- Ein öffentlich signiertes CA-Zertifikat verwenden. Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat verwenden, können Sie die Grid-Management-API verwenden, um die Zertifikatrotation zu automatisieren. So können Sie bald abgelaufene Zertifikate unterbrechungsfrei ersetzen.
- Wenn Sie ein selbstsigniertes StorageGRID-Zertifikat generiert haben und dieses Zertifikat kurz vor dem Ablauf steht, müssen Sie das Zertifikat sowohl in StorageGRID als auch in ONTAP manuell ersetzen,

bevor das vorhandene Zertifikat abläuft. Wenn ein selbstsigniertes Zertifikat bereits abgelaufen ist, deaktivieren Sie die Zertifikatvalidierung in ONTAP, um einen Zugriffsverlust zu verhindern.

Siehe ["NetApp Knowledge Base: So konfigurieren Sie ein neues selbstsigniertes StorageGRID Serverzertifikat für eine vorhandene ONTAP FabricPool Implementierung"](#) Weitere Anweisungen.

## Best Practices für die Verwendung von ILM mit FabricPool-Daten

Wenn Sie FabricPool für das Tiering von Daten für StorageGRID verwenden, müssen Sie die Anforderungen für die Verwendung von StorageGRID Information Lifecycle Management (ILM) mit FabricPool-Daten kennen.



FabricPool ist nicht mit den StorageGRID ILM-Regeln oder -Richtlinien bekannt. Wenn die StorageGRID ILM-Richtlinie falsch konfiguriert ist, kann es zu Datenverlusten kommen. Ausführliche Informationen finden Sie unter ["Erstellen Sie eine ILM-Regel: Überblick"](#) Und ["Erstellen Sie eine ILM-Richtlinie: Überblick"](#).

### Richtlinien für die Verwendung von ILM mit FabricPool

Wenn Sie den FabricPool-Einrichtungsassistenten verwenden, erstellt der Assistent automatisch eine neue ILM-Regel für jeden von Ihnen erstellten S3-Bucket und fügt diese Regel einer inaktiven Richtlinie hinzu. Sie werden aufgefordert, die Richtlinie zu aktivieren. Die automatisch erstellte Regel folgt den empfohlenen Best Practices: Sie verwendet 2+1 Erasure Coding an einem einzigen Standort.

Wenn Sie StorageGRID manuell konfigurieren und nicht den FabricPool Setup-Assistenten verwenden, lesen Sie diese Richtlinien, um sicherzustellen, dass Ihre ILM-Regeln und ILM-Richtlinien für FabricPool-Daten und Ihre Geschäftsanforderungen geeignet sind. Möglicherweise müssen Sie neue Regeln erstellen und Ihre aktiven ILM-Richtlinien aktualisieren, um diese Richtlinien zu erfüllen.

- Sie können jede beliebige Kombination aus Replizierung und Verfahren zur Einhaltung von Datenkonsistenz zum Schutz von Cloud-Tiering-Daten verwenden.

Die empfohlene Best Practice besteht darin, ein 2+1-Verfahren zur Einhaltung von Datenkonsistenz an einem Standort zu verwenden, um eine kosteneffiziente Datensicherung zu gewährleisten. Das Verfahren zur Einhaltung von Datenkonsistenz benötigt zwar mehr CPU, bietet aber wesentlich weniger Storage-Kapazität als Replizierung. Die Schemata 4+1 und 6+1 benötigen weniger Kapazität als das Schema 2+1. Die Schemata 4+1 und 6+1 sind jedoch weniger flexibel, wenn Sie während der Grid-Erweiterung Storage-Nodes hinzufügen müssen. Weitere Informationen finden Sie unter ["Erweitern Sie Storage-Kapazität für Objekte, die nach dem Erasure-Coding-Verfahren codiert wurden"](#).

- Jede auf FabricPool-Daten angewandte Regel muss entweder Erasure Coding verwenden oder mindestens zwei replizierte Kopien erstellen.



Eine ILM-Regel, die immer nur eine replizierte Kopie erstellt, gefährdet Daten permanent. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

- Wenn es nötig ist ["FabricPool-Daten aus StorageGRID entfernen"](#), Verwenden Sie ONTAP, um alle Daten

für das FabricPool-Volume abzurufen und auf die Performance-Tier zu übertragen.



Verwenden Sie zur Vermeidung von Datenverlust keine ILM-Regel, die ausläuft oder die Cloud-Tiering-Daten von FabricPool löscht. Legen Sie den Aufbewahrungszeitraum in jeder ILM-Regel auf **Forever** fest, um sicherzustellen, dass FabricPool Objekte nicht durch StorageGRID ILM gelöscht werden.

- Erstellen Sie keine Regeln, um Daten aus FabricPool Cloud-Tiers an einen anderen Speicherort zu verschieben. Sie können keinen Cloud-Speicherpool verwenden, um FabricPool-Daten in einen anderen Objektspeicher zu verschieben. Ebenso können Sie FabricPool-Daten nicht mit einem Archivknoten auf Band archivieren.



Die Verwendung von Cloud Storage Pools mit FabricPool wird nicht unterstützt, weil die zusätzliche Latenz zum Abrufen eines Objekts aus dem Cloud-Storage-Pool-Ziel hinzugefügt wird.

- Ab ONTAP 9.8 können Sie optional Objekt-Tags erstellen, um Daten in Tiers zu klassifizieren und zu sortieren und das Management zu erleichtern. Beispielsweise können Sie Tags nur auf FabricPool Volumes festlegen, die an StorageGRID angebunden sind. Wenn Sie dann ILM-Regeln in StorageGRID erstellen, können Sie diese Daten mithilfe des erweiterten Filter Object Tag auswählen und platzieren.

## Weitere Best Practices für StorageGRID und FabricPool

Wenn Sie ein StorageGRID-System für die Verwendung mit FabricPool konfigurieren, müssen Sie möglicherweise andere StorageGRID-Optionen ändern. Bevor Sie eine globale Einstellung ändern, überlegen Sie, wie sich die Änderung auf andere S3-Anwendungen auswirkt.

### Überwachungsmeldung und Protokollziele

FabricPool-Workloads verfügen oft über eine hohe Rate an Lesevorgängen, die ein hohes Volumen an Audit-Nachrichten erzeugen können.

- Wenn Sie keine Aufzeichnung von Client-Leseoperationen für FabricPool oder eine andere S3-Anwendung benötigen, gehen Sie optional zu **CONFIGURATION > Monitoring > Audit und Syslog-Server**. Ändern Sie die Einstellung **Client reads** auf **Error**, um die Anzahl der im Auditprotokoll aufgezeichneten Überwachungsmeldungen zu verringern. Siehe "[Konfigurieren von Überwachungsmeldungen und Protokollzielen](#)" Entsprechende Details.
- Wenn Sie über ein großes Grid verfügen, mehrere Arten von S3-Applikationen verwenden oder alle Audit-Daten behalten möchten, konfigurieren Sie einen externen Syslog-Server und speichern Sie Audit-Informationen Remote. Durch die Verwendung eines externen Servers werden die Auswirkungen der Protokollierung von Audit-Nachrichten auf die Performance minimiert, ohne dass die Vollständigkeit der Audit-Daten reduziert wird. Siehe "[Überlegungen für externen Syslog-Server](#)" Entsprechende Details.

### Objektverschlüsselung

Beim Konfigurieren von StorageGRID können Sie optional den aktivieren "[Globale Option für Verschlüsselung gespeicherter Objekte](#)" Falls Datenverschlüsselung für andere StorageGRID Clients erforderlich ist. Die Daten, die von FabricPool zu StorageGRID verschoben werden, sind bereits verschlüsselt, d. h. die Aktivierung der StorageGRID-Einstellung ist nicht erforderlich. Die Client-seitige Verschlüsselung ist Eigentum von ONTAP.

## Objektkomprimierung

Aktivieren Sie beim Konfigurieren von StorageGRID nicht das "[Globale Option zum Komprimieren gespeicherter Objekte](#)". Die Daten, die von FabricPool zu StorageGRID verschoben werden, werden bereits komprimiert. Durch Verwendung der Option StorageGRID wird die Größe eines Objekts nicht weiter reduziert.

## Bucket-Konsistenz

Für FabricPool-Buckets lautet die empfohlene Bucket-Konsistenz **Read-after-New-write**, was die Standardkonsistenz für einen neuen Bucket ist. Bearbeiten Sie FabricPool Buckets nicht, um **available** oder **strong-site** zu verwenden.

## FabricPool Tiering

Wenn ein StorageGRID Node Storage verwendet, der von einem NetApp ONTAP System zugewiesen wurde, vergewissern Sie sich, dass auf dem Volume keine FabricPool-Tiering-Richtlinie aktiviert ist. Wenn beispielsweise ein StorageGRID Node auf einem VMware Host ausgeführt wird, stellen Sie sicher, dass für das Volume, das den Datastore für den StorageGRID Node unterstützt, keine FabricPool-Tiering-Richtlinie aktiviert ist. Das Deaktivieren von FabricPool Tiering für Volumes, die in Verbindung mit StorageGRID Nodes verwendet werden, vereinfacht die Fehlerbehebung und Storage-Vorgänge.



Verwenden Sie FabricPool niemals, um StorageGRID-bezogene Daten in das Tiering zurück zu StorageGRID selbst zu verschieben. Das Tiering von StorageGRID-Daten zurück in die StorageGRID verbessert die Fehlerbehebung und reduziert die Komplexität von betrieblichen Abläufen.

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.