



StorageGRID Best Practices für FabricPool

StorageGRID software

NetApp
July 23, 2026

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

Inhalt

StorageGRID Best Practices für FabricPool	1
Bewährte Verfahren für StorageGRID Hochverfügbarkeitsgruppen (HA) mit FabricPool	1
Was ist eine HA-Gruppe?	1
Verwendung von HA-Gruppen	1
Bewährte Verfahren für den StorageGRID-Lastausgleich mit FabricPool	1
Bewährte Methoden für den Mandantenzugriff auf den Lastausgleichs-Endpunkt, der für FabricPool verwendet wird	2
Bewährte Verfahren für das Sicherheitszertifikat	2
Bewährte Verfahren für die Verwendung von StorageGRID ILM mit FabricPool Daten	3
Richtlinien für die Verwendung von ILM mit FabricPool	3
Bewährte Methoden für StorageGRID globale Einstellungen mit FabricPool	4
Ziele für Revisionsmeldungen und Revisionsprotokolle	4
Objektverschlüsselung	4
Objektkomprimierung	5
S3 Object Lock	5
Bucket-Konsistenz	5
FabricPool Tiering	5

StorageGRID Best Practices für FabricPool

Bewährte Verfahren für StorageGRID Hochverfügbarkeitsgruppen (HA) mit FabricPool

Bevor StorageGRID als FabricPool Cloud-Tier angebunden wird, empfiehlt sich eine Information über StorageGRID Hochverfügbarkeitsgruppen (HA-Gruppen) sowie eine Überprüfung der Best Practices für die Nutzung von HA-Gruppen mit FabricPool.

Was ist eine HA-Gruppe?

Eine Hochverfügbarkeitsgruppe (HA-Gruppe) ist eine Sammlung von Schnittstellen mehrerer StorageGRID Gateway Nodes, Admin Nodes oder beider. Eine HA-Gruppe trägt dazu bei, die Verfügbarkeit von Client-Datenverbindungen aufrechtzuerhalten. Fällt die aktive Schnittstelle in der HA-Gruppe aus, kann eine Backup-Schnittstelle die Arbeitslast mit minimalen Auswirkungen auf FabricPool-Operationen übernehmen.

Jede HA-Gruppe bietet hochverfügbaren Zugriff auf die gemeinsam genutzten Dienste der zugehörigen Knoten. Beispielsweise bietet eine HA-Gruppe, die nur Schnittstellen auf Gateway Nodes oder sowohl auf Admin Nodes als auch auf Gateway Nodes umfasst, hochverfügbaren Zugriff auf den gemeinsam genutzten Load Balancer Service.

Weitere Informationen zu Hochverfügbarkeitsgruppen sind unter ["Hochverfügbarkeitsgruppen \(HA\) verwalten"](#) zu finden.

Verwendung von HA-Gruppen

Die besten Vorgehensweisen zum Erstellen einer StorageGRID HA-Gruppe für FabricPool hängen von der Arbeitslast ab.

- Wenn Sie planen, FabricPool mit primären Arbeitslastdaten zu verwenden, muss eine HA-Gruppe erstellt werden, die mindestens zwei Lastausgleichsknoten umfasst, um Unterbrechungen beim Datenabruf zu verhindern.
- Wenn die FabricPool Snapshot-only Volume Tiering-Richtlinie oder nicht-primäre lokale Performance-Tiers (zum Beispiel Disaster-Recovery-Standorte oder NetApp SnapMirror® Ziele) verwendet werden, kann eine HA-Gruppe mit nur einem Knoten konfiguriert werden.

Diese Anleitung beschreibt die Einrichtung einer HA-Gruppe für Active-Backup HA (ein Knoten ist aktiv und ein Knoten dient als Backup). Es besteht jedoch die Möglichkeit, stattdessen DNS Round Robin oder Active-Active HA zu verwenden. Die Vorteile dieser anderen HA-Konfigurationen sind unter ["Konfigurationsoptionen für HA-Gruppen"](#) aufgeführt.

Bewährte Verfahren für den StorageGRID-Lastausgleich mit FabricPool

Vor dem Anbinden von StorageGRID als FabricPool Cloud-Tier empfiehlt sich eine Überprüfung der Best Practices für die Verwendung von Lastausgleichern mit FabricPool.

Allgemeine Informationen zum StorageGRID Lastausgleich und zum Lastausgleichszertifikat sind unter ["Überlegungen zum Lastausgleich"](#) zu finden.

Bewährte Methoden für den Mandantenzugriff auf den Lastausgleichs-Endpunkt, der für FabricPool verwendet wird

Sie können steuern, welche Mandanten einen bestimmten Lastausgleich-Endpunkt für den Zugriff auf ihre Buckets verwenden können. Es kann allen Mandanten erlaubt werden, einigen Mandanten erlaubt werden oder einigen Mandanten der Zugriff verweigert werden. Beim Erstellen eines Lastausgleich-Endpunkts für die FabricPool-Nutzung ist **Alle Mandanten zulassen** auszuwählen. ONTAP verschlüsselt die Daten, die in StorageGRID Buckets abgelegt werden, sodass durch diese zusätzliche Sicherheitsebene nur wenig zusätzlicher Schutz geboten wird.

Bewährte Verfahren für das Sicherheitszertifikat

Wenn ein StorageGRID Load Balancer Endpoint für die FabricPool-Verwendung erstellt wird, wird das Sicherheitszertifikat bereitgestellt, das ONTAP die Authentifizierung mit StorageGRID ermöglicht.

In den meisten Fällen sollte die Verbindung zwischen ONTAP und StorageGRID die Transport Layer Security (TLS)-Verschlüsselung verwenden. Die Verwendung von FabricPool ohne TLS-Verschlüsselung wird unterstützt, ist jedoch nicht empfehlenswert. Beim Auswählen des Netzwerkprotokolls für den StorageGRID Lastausgleichs-Endpunkt ist **HTTPS** auszuwählen. Anschließend ist das Sicherheitszertifikat bereitzustellen, das ONTAP die Authentifizierung bei StorageGRID ermöglicht.

Weitere Informationen zum Serverzertifikat für einen Lastausgleich-Endpunkt:

- ["Sicherheitszertifikate verwalten"](#)
- ["Überlegungen zum Lastausgleich"](#)
- ["Richtlinien zur Härtung von Serverzertifikaten"](#)

Zertifikat zu ONTAP hinzufügen

Wenn Sie StorageGRID als FabricPool Cloud-Tier hinzufügen, muss dasselbe Zertifikat auf dem ONTAP Cluster installiert werden, einschließlich des Stammzertifikats und aller untergeordneten Zertifizierungsstellen (CA) Zertifikate.

Zertifikatsablauf verwalten



Wenn das Zertifikat, das zur Sicherung der Verbindung zwischen ONTAP und StorageGRID verwendet wird, abläuft, wird FabricPool vorübergehend nicht mehr funktionieren und ONTAP verliert vorübergehend den Zugriff auf die zu StorageGRID ausgelagerten Daten.

Um Probleme mit abgelaufenen Zertifikaten zu vermeiden, sind diese bewährten Vorgehensweisen zu beachten:

- Alle Warnmeldungen, die auf bevorstehende Ablaufdaten von Zertifikaten hinweisen, wie zum Beispiel die Warnmeldungen **Expiration of load balancer endpoint certificate** und **Expiration of global server certificate for S3 API**, sollten sorgfältig überwacht werden.
- Die StorageGRID und ONTAP Versionen des Zertifikats sollten stets synchron gehalten werden. Wird das für einen Lastausgleich-Endpunkt verwendete Zertifikat ersetzt oder erneuert, ist auch das entsprechende von ONTAP für die Cloud-Tier verwendete Zertifikat zu ersetzen oder zu erneuern.
- Ein öffentlich signiertes CA-Zertifikat verwenden. Bei Verwendung eines von einer CA signierten Zertifikats kann die Grid Management API zur Automatisierung der Zertifikatsrotation eingesetzt werden. So lassen sich Zertifikate, die bald ablaufen, ohne Unterbrechung ersetzen.

- Wenn Sie ein selbstsigniertes StorageGRID-Zertifikat erstellt haben und dieses demnächst abläuft, muss das Zertifikat sowohl in StorageGRID als auch in ONTAP manuell ersetzt werden, bevor das bestehende Zertifikat abläuft. Ist ein selbstsigniertes Zertifikat bereits abgelaufen, sollte die Zertifikatsvalidierung in ONTAP deaktiviert werden, um Zugriffsverluste zu vermeiden.

Siehe ["NetApp Knowledge Base: Konfiguration eines neuen selbstsignierten StorageGRID-Serverzertifikats auf einer bestehenden ONTAP FabricPool Bereitstellung"](#) für Anweisungen.

Bewährte Verfahren für die Verwendung von StorageGRID ILM mit FabricPool Daten

Wenn Sie FabricPool verwenden, um Daten auf StorageGRID zu verschieben, müssen Sie die Anforderungen für die Verwendung von StorageGRID Information Lifecycle Management (ILM) mit FabricPool-Daten kennen.



FabricPool hat keine Kenntnis von StorageGRID ILM-Regeln oder -Richtlinien. Datenverlust kann auftreten, wenn die StorageGRID ILM-Richtlinie falsch konfiguriert ist. Ausführliche Informationen finden sich unter ["ILM-Regeln zur Verwaltung von Objekten verwenden"](#) und ["ILM-Richtlinien erstellen"](#).

Richtlinien für die Verwendung von ILM mit FabricPool

Wenn der FabricPool Setup-Assistent verwendet wird, erstellt der Assistent automatisch für jeden erstellten S3-Bucket eine neue ILM-Regel und fügt diese einer inaktiven Richtlinie hinzu. Es erfolgt eine Aufforderung, die Richtlinie zu aktivieren. Die automatisch erstellte Regel entspricht den empfohlenen Best Practices: Sie verwendet 2+1 Erasure Coding an einem einzelnen Standort.

Wenn StorageGRID manuell statt mit dem FabricPool Setup-Assistenten konfiguriert wird, sollten diese Richtlinien geprüft werden, um sicherzustellen, dass die ILM-Regeln und die ILM-Richtlinie für FabricPool Daten und die geschäftlichen Anforderungen geeignet sind. Möglicherweise ist es erforderlich, neue Regeln zu erstellen und die aktiven ILM-Richtlinien zu aktualisieren, um diese Vorgaben zu erfüllen.

- Sie können beliebige Kombinationen von Replikations- und Erasure-Codierungsregeln verwenden, um Cloud-Tier-Daten zu schützen.

Die empfohlene Best Practice ist die Verwendung von 2+1 Erasure Coding innerhalb eines Standorts für kosteneffizienten Datenschutz. Erasure Coding benötigt mehr CPU, bietet jedoch deutlich weniger Speicherkapazität als Replikation. Die 4+1- und 6+1-Verfahren benötigen weniger Kapazität als das 2+1-Verfahren. Allerdings sind die 4+1- und 6+1-Verfahren weniger flexibel, falls während einer Grid-Erweiterung Speicherknoten hinzugefügt werden müssen. Weitere Details finden sich unter ["Speicherkapazität für mit Löschkodierung versehene Objekte hinzufügen"](#).

- Jede auf FabricPool Daten angewendete Regel muss entweder eine Löschungscodierung verwenden oder mindestens zwei replizierte Kopien erstellen.



Eine ILM-Regel, die nur eine replizierte Kopie für einen beliebigen Zeitraum erstellt, setzt Daten dem Risiko eines dauerhaften Datenverlusts aus. Existiert nur eine replizierte Kopie eines Objekts, geht dieses Objekt verloren, wenn ein Storage Node ausfällt oder einen schwerwiegenden Fehler aufweist. Auch während Wartungsarbeiten wie Upgrades ist der Zugriff auf das Objekt vorübergehend nicht möglich.

- Falls Sie ["Entfernen von FabricPool-Daten aus StorageGRID"](#) benötigen, kann ONTAP verwendet werden, um alle Daten für das FabricPool Volume abzurufen und in die Performance-Ebene zu verschieben.



Um Datenverlust zu vermeiden, sollte keine ILM-Regel verwendet werden, die FabricPool Cloud-Tier-Daten ablaufen lässt oder löscht. Die Aufbewahrungsdauer ist in jeder ILM-Regel auf **unbegrenzt** festzulegen, damit FabricPool Objekte nicht von StorageGRID ILM gelöscht werden.

- Es sollten keine Regeln erstellt werden, die FabricPool Cloud-Tier-Daten aus dem Bucket an einen anderen Speicherort verschieben. Ein Cloud Storage Pool kann nicht verwendet werden, um FabricPool Daten in einen anderen Objektspeicher zu verschieben.



Die Verwendung von Cloud Storage Pools mit FabricPool wird aufgrund der zusätzlichen Latenz beim Abrufen eines Objekts vom Cloud Storage Pool-Ziel nicht unterstützt.

- Ab ONTAP 9.8 können optional Objekttags erstellt werden, um gestaffelte Daten zur einfacheren Verwaltung zu klassifizieren und zu sortieren. Beispielsweise können Tags nur auf FabricPool Volumes festgelegt werden, die an StorageGRID angebunden sind. Wenn ILM-Regeln in StorageGRID erstellt werden, kann der erweiterte Filter „Objektag“ verwendet werden, um diese Daten auszuwählen und zu platzieren.

Bewährte Methoden für StorageGRID globale Einstellungen mit FabricPool

Bei der Konfiguration eines StorageGRID Systems für die Verwendung mit FabricPool kann es erforderlich sein, weitere StorageGRID Optionen zu ändern. Vor einer Änderung einer globalen Einstellung sollte berücksichtigt werden, wie sich diese Änderung auf andere S3 Applikationen auswirkt.

Ziele für Revisionsmeldungen und Revisionsprotokolle

FabricPool Arbeitslasten weisen häufig eine hohe Anzahl von Lesevorgängen auf, was zu einem hohen Volumen an Revisionsmeldungen führen kann.

- Wenn kein Protokoll der Client-Lesevorgänge für FabricPool oder eine andere S3-Applikation benötigt wird, kann optional zu **Konfiguration > Überwachung > Audit und Syslog-Server** gewechselt werden. Die Einstellung **Client-Lesevorgänge** kann auf **Fehler** geändert werden, um die Anzahl der im Revisionsprotokoll aufgezeichneten Audit-Meldungen zu verringern. Siehe ["Logverwaltung und externen Syslog-Server konfigurieren"](#) für Details.
- Wenn ein großes Grid vorhanden ist, mehrere Typen von S3-Anwendungen verwendet werden oder alle Revisionsdaten aufbewahrt werden sollen, empfiehlt sich die Konfiguration eines externen Syslog-Servers und das Speichern der Revisionsinformationen extern. Die Nutzung eines externen Servers minimiert die Auswirkungen der Protokollierung von Revisionsmeldungen auf die Performance, ohne die Vollständigkeit der Revisionsdaten zu verringern. Siehe ["Überlegungen zum externen Syslog-Server"](#) für Details.

Objektverschlüsselung

Bei der Konfiguration von StorageGRID kann optional die ["Globale Option für die Verschlüsselung gespeicherter Objekte"](#) aktiviert werden, wenn eine Datenverschlüsselung für andere StorageGRID Clients erforderlich ist. Die von FabricPool zu StorageGRID ausgelagerten Daten sind bereits verschlüsselt, daher ist

die Aktivierung der StorageGRID-Einstellung nicht erforderlich. Die clientseitigen Verschlüsselungsschlüssel gehören ONTAP.

Objektkomprimierung

Aktivieren Sie bei der Konfiguration von StorageGRID die Option "[Globale Option zum Komprimieren gespeicherter Objekte](#)" nicht. Die von FabricPool zu StorageGRID ausgelagerten Daten sind bereits komprimiert. Die Verwendung der StorageGRID Option reduziert die Größe eines Objekts nicht weiter.

S3 Object Lock

Wenn die globale S3 Object Lock-Einstellung für Ihr StorageGRID System aktiviert ist, "[S3 Object Lock](#)" nicht aktivieren, wenn FabricPool Buckets erstellt werden. S3 Object Lock wird für FabricPool Buckets nicht unterstützt.

Bucket-Konsistenz

Für FabricPool Buckets wird die Bucket-Konsistenz **Read-after-new-write** empfohlen, was die Standardkonsistenz für einen neuen Bucket ist. FabricPool Buckets sollten nicht so bearbeitet werden, dass **Available** oder **Strong-site** verwendet wird.

FabricPool Tiering

Wenn ein StorageGRID Knoten Speicher nutzt, der von einem NetApp ONTAP System zugewiesen wurde, ist sicherzustellen, dass für das Volume keine FabricPool Tiering-Richtlinie aktiviert ist. Wenn ein StorageGRID Knoten beispielsweise auf einem VMware Host ausgeführt wird, ist sicherzustellen, dass für das Volume, das den Datenspeicher des StorageGRID Knotens bereitstellt, keine FabricPool Tiering-Richtlinie aktiviert ist. Das Deaktivieren des FabricPool Tierings für Volumes, die mit StorageGRID Knoten verwendet werden, vereinfacht die Fehlersuche und den Speicherbetrieb.



Es sollte niemals FabricPool verwendet werden, um Daten, die mit StorageGRID in Zusammenhang stehen, wieder auf StorageGRID selbst zu verschieben. Das Tiering von StorageGRID-Daten zurück auf StorageGRID erhöht die Komplexität bei der Fehlerbehebung und im Betrieb.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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.