



StorageGRID mit FabricPool

StorageGRID software

NetApp
July 23, 2026

Inhalt

StorageGRID mit FabricPool	1
Konfigurationsworkflow für die Verwendung von StorageGRID mit FabricPool	1
Kurzanleitung zur Konfiguration von StorageGRID für FabricPool	1
Was ist FabricPool?	2
Was ist StorageGRID?	2
Warum StorageGRID als FabricPool Cloud-Tier verwenden?	2
Informationen, die benötigt werden, um StorageGRID als FabricPool Cloud-Tier anzubinden	3
Welche Werte werden benötigt?	3
Wie erhalte ich diese Werte?	3
Den FabricPool Einrichtungsassistenten verwenden	4
Erfahren Sie mehr über den StorageGRID FabricPool Einrichtungsassistenten	4
Greifen Sie auf den StorageGRID FabricPool Einrichtungsassistenten zu und schließen Sie ihn ab	6
StorageGRID manuell konfigurieren	18
Erstellen Sie eine Hochverfügbarkeitsgruppe (HA) für FabricPool in StorageGRID	18
Erstellen Sie einen Load-Balancer-Endpunkt für FabricPool in StorageGRID	20
Erstellen Sie ein Mandantenkonto für FabricPool in StorageGRID	22
Erstellen Sie einen S3-Bucket und rufen Sie Zugriffsschlüssel für FabricPool in StorageGRID ab	24
StorageGRID ILM für FabricPool-Daten konfigurieren	25
Erstellen Sie eine Richtlinie zur Verkehrsklassifizierung für FabricPool in StorageGRID	27
Konfigurieren Sie ONTAP System Manager, um StorageGRID als FabricPool Cloud-Tier hinzuzufügen	29
Auf ONTAP System Manager zugreifen	29
StorageGRID-Werte eingeben	29
Konfigurieren Sie DNS-Servereinträge für StorageGRID mit FabricPool	31
DNS-Einträge für StorageGRID Servernamen	31
DNS-Einträge für virtuelle Hosted-Style-Anfragen	31
StorageGRID Best Practices für FabricPool	31
Bewährte Verfahren für StorageGRID Hochverfügbarkeitsgruppen (HA) mit FabricPool	31
Bewährte Verfahren für den StorageGRID-Lastausgleich mit FabricPool	32
Bewährte Verfahren für die Verwendung von StorageGRID ILM mit FabricPool Daten	33
Bewährte Methoden für StorageGRID globale Einstellungen mit FabricPool	35
Entfernen von FabricPool Daten aus StorageGRID	36

StorageGRID mit FabricPool

Konfigurationsworkflow für die Verwendung von StorageGRID mit FabricPool

Wenn Sie NetApp ONTAP Software verwenden, kann NetApp FabricPool genutzt werden, um inaktive Daten in ein NetApp StorageGRID Objektspeicher-System zu verschieben.

Diese Anweisungen dienen dazu:

- Es werden die Überlegungen und Best Practices für die Konfiguration von StorageGRID für eine FabricPool-Arbeitslast dargestellt.
- Es wird beschrieben, wie ein StorageGRID Objektspeichersystem für die Verwendung mit FabricPool konfiguriert wird.
- Es wird erläutert, wie die erforderlichen Werte für ONTAP bereitgestellt werden, wenn StorageGRID als FabricPool Cloud-Tier angebunden wird.

Kurzanleitung zur Konfiguration von StorageGRID für FabricPool

1

Konfiguration planen

- Entscheiden Sie, welche FabricPool Volume-Tiering-Richtlinie für die Tiering von inaktiven ONTAP Daten zu StorageGRID verwendet wird.
- Ein StorageGRID System wird geplant und installiert, um den Anforderungen an Speicherkapazität und Performance zu entsprechen.
- Mit der StorageGRID Systemsoftware vertraut machen, einschließlich der ["Grid Manager"](#) und der ["Tenant Manager"](#).
- Die FabricPool Best Practices für ["HA-Gruppen"](#), ["\\${post_edited_translations.segment}"](#), ["ILM"](#) und ["mehr"](#) werden dargestellt.
- Diese zusätzlichen Ressourcen bieten Einzelheiten zur Verwendung und Konfiguration von ONTAP und FabricPool:

["TR-4598: FabricPool Best Practices in ONTAP"](#)

["ONTAP Dokumentation für FabricPool"](#)

2

Führen Sie die erforderlichen Aufgaben aus

Beziehen von ["Informationen, die benötigt werden, um StorageGRID als Cloud-Tier anzubinden"](#), einschließlich:

- IP-Adressen
- Domainnamen
- SSL-Zertifikat

Optional kann "Identitätsföderation" und "Single Sign-On" konfiguriert werden.

3

StorageGRID-Einstellungen konfigurieren

`${post_edited_translations.segment}`

Die Verwendung des "FabricPool Einrichtungsassistent" ist die empfohlene und schnellste Methode, um alle Elemente zu konfigurieren, aber es besteht auch die Möglichkeit, jede Entität bei Bedarf manuell zu konfigurieren.

4

ONTAP und DNS konfigurieren

Verwenden Sie ONTAP, um "eine Cloud-Ebene hinzufügen", das die StorageGRID Werte verwendet. Danach "DNS-Einträge konfigurieren", um IP-Adressen mit den Domännennamen zu verknüpfen, die Sie verwenden möchten.

5

Überwachen und verwalten

Sobald Ihr System eingerichtet und betriebsbereit ist, werden in ONTAP und StorageGRID fortlaufende Aufgaben ausgeführt, um die FabricPool Datenschichtung im Laufe der Zeit zu verwalten und zu überwachen.

Was ist FabricPool?

FabricPool ist eine ONTAP Hybrid-Speicherlösung, die ein leistungsstarkes Flash-Aggregat als Performance-Tier und einen Objektspeicher als Cloud-Tier verwendet. Die Nutzung von FabricPool-fähigen Aggregaten trägt dazu bei, die Speicherkosten zu senken, ohne die Leistung, Effizienz oder den Schutz zu beeinträchtigen.

FabricPool verknüpft eine Cloud-Ebene (einen externen Objektspeicher wie StorageGRID) mit einer lokalen Ebene (einem ONTAP Storage-Aggregat), um eine zusammengesetzte Sammlung von Datenträgern zu erstellen. Volumes innerhalb der FabricPool können dann die Vorteile des Tierings nutzen, indem aktive (heiße) Daten auf Hochleistungsspeicher (der lokalen Ebene) gehalten und inaktive (kalte) Daten auf den externen Objektspeicher (die Cloud-Ebene) ausgelagert werden.

`${post_edited_translations.segment}`

Was ist StorageGRID?

NetApp StorageGRID ist eine Speicherarchitektur, die Daten als Objekte verwaltet, im Gegensatz zu anderen Speicherarchitekturen wie Datei- oder Blockspeicher. Objekte werden in einem einzelnen Container (wie einem Bucket) aufbewahrt und sind nicht als Dateien in einem Verzeichnis innerhalb anderer Verzeichnisse verschachtelt. Obwohl Objektspeicher im Allgemeinen eine geringere Leistung als Datei- oder Blockspeicher bietet, ist er deutlich skalierbarer. StorageGRID Buckets können Petabytes an Daten und Milliarden von Objekten aufnehmen.

Warum StorageGRID als FabricPool Cloud-Tier verwenden?

FabricPool kann ONTAP-Daten auf eine Reihe von Objektspeicheranbietern, einschließlich StorageGRID, verschieben. Im Gegensatz zu öffentlichen Clouds, die möglicherweise eine maximale Anzahl unterstützter Input/Output-Operationen pro Sekunde (IOPS) auf Bucket- oder Containerebene festlegen, skaliert die StorageGRID-Leistung mit der Anzahl der Knoten im System. Die Nutzung von StorageGRID als FabricPool Cloud-Tier ermöglicht es, kalte Daten in der eigenen privaten Cloud zu speichern, was höchste Leistung und

vollständige Kontrolle über die Daten bietet.

Darüber hinaus ist für FabricPool keine Lizenz erforderlich, wenn StorageGRID als Cloud-Tier verwendet wird.

Informationen, die benötigt werden, um StorageGRID als FabricPool Cloud-Tier anzubinden

Bevor Sie StorageGRID als Cloud-Tier für FabricPool anbinden können, müssen in StorageGRID Konfigurationsschritte durchgeführt und bestimmte Werte für die Verwendung in ONTAP ermittelt werden.

Welche Werte werden benötigt?

Die folgende Tabelle zeigt die Werte, die Sie in StorageGRID konfigurieren müssen, und wie diese Werte von ONTAP und dem DNS-Server verwendet werden.

Wert	Wo der Wert konfiguriert wird	Wo Wert verwendet wird
Virtuelle IP-Adressen (VIP)	StorageGRID > HA-Gruppe	DNS-Eintrag
Port	StorageGRID > Load Balancer Endpoint	ONTAP System Manager > Cloud-Tier hinzufügen
SSL-Zertifikat	StorageGRID > Load Balancer Endpoint	ONTAP System Manager > Cloud-Tier hinzufügen
Servername (FQDN)	StorageGRID > Load Balancer Endpoint	DNS-Eintrag
Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel	<code>\${post_edited_translations.segment}</code>	ONTAP System Manager > Cloud-Tier hinzufügen
Bucket/Container-Name	<code>\${post_edited_translations.segment}</code>	ONTAP System Manager > Cloud-Tier hinzufügen

Wie erhalte ich diese Werte?

`${post_edited_translations.segment}`

- Verwenden Sie den ["FabricPool Einrichtungsassistent"](#). Der FabricPool Setup-Assistent unterstützt Sie dabei, die erforderlichen Werte in StorageGRID schnell zu konfigurieren und gibt eine Datei aus, die zur Konfiguration von ONTAP System Manager verwendet werden kann. Der Assistent führt durch die erforderlichen Schritte und hilft dabei, sicherzustellen, dass die Einstellungen den Best Practices von StorageGRID und FabricPool entsprechen.
- Jedes Element wird manuell konfiguriert. Anschließend werden die Werte in ONTAP System Manager oder die ONTAP CLI eingegeben. Dabei sind folgende Schritte zu beachten:
 - a. ["Eine Hochverfügbarkeitsgruppe \(HA-Gruppe\) für FabricPool konfigurieren"](#).
 - b. ["Einen Load Balancer-Endpoint für FabricPool erstellen"](#).

- c. ["Ein Mandantenkonto für FabricPool erstellen"](#).
- d. Melden Sie sich beim Mieterkonto an und ["Den Bucket und die Zugriffsschlüssel für den Root-Benutzer erstellen"](#).
- e. Erstellen Sie eine ILM-Regel für FabricPool Daten und fügen Sie sie zu Ihren aktiven ILM-Richtlinien hinzu. Siehe ["ILM für FabricPool Daten konfigurieren"](#).
- f. Optional, ["eine Verkehrsklassifizierungsrichtlinie für FabricPool erstellen"](#).

Den FabricPool Einrichtungsassistenten verwenden

Erfahren Sie mehr über den StorageGRID FabricPool Einrichtungsassistenten

Sie können den FabricPool Einrichtungsassistenten verwenden, um StorageGRID als Objektspeichersystem für eine FabricPool Cloud-Ebene zu konfigurieren. Nach Abschluss des Einrichtungsassistenten lassen sich die erforderlichen Details im ONTAP System Manager eingeben.

Wann der FabricPool Setup-Assistent verwendet wird

Der FabricPool Setup-Assistent führt durch jeden Schritt der Konfiguration von StorageGRID für die Verwendung mit FabricPool und konfiguriert dabei bestimmte Entitäten wie ILM und Richtlinien zur Datenverkehrsklassifizierung automatisch. Im Rahmen des Abschlusses des Assistenten wird eine Datei heruntergeladen, die zur Eingabe von Werten in den ONTAP System Manager verwendet werden kann. Mit dem Assistenten lässt sich das System schneller konfigurieren und es wird sichergestellt, dass die Einstellungen den Best Practices von StorageGRID und FabricPool entsprechen.

Sofern Sie über Root-Zugriffsrechte verfügen, kann der FabricPool Setup-Assistent beim ersten Start des StorageGRID Grid Managers abgeschlossen werden oder zu einem späteren Zeitpunkt aufgerufen und abgeschlossen werden. Abhängig von Ihren Anforderungen ist es auch möglich, einige oder alle erforderlichen Elemente manuell zu konfigurieren und anschließend den Assistenten zu verwenden, um die von ONTAP benötigten Werte in einer einzigen Datei zusammenzustellen.



Der FabricPool Setup-Assistent sollte verwendet werden, es sei denn, es sind spezielle Anforderungen bekannt oder die Implementierung erfordert erhebliche Anpassungen.

Bevor der Assistent verwendet wird

Bestätigen Sie, dass diese erforderlichen Schritte abgeschlossen wurden.

Bewährte Verfahren im Überblick

- Sie haben ein allgemeines Verständnis von ["Informationen, die benötigt werden, um StorageGRID als Cloud-Tier anzubinden"](#).
- Sie haben die FabricPool Best Practices für Folgendes geprüft:
 - ["Hochverfügbarkeitsgruppen \(HA\)"](#)
 - ["Lastverteilung"](#)
 - ["ILM-Regeln und Richtlinien"](#)

IP-Adressen beziehen und VLAN-Schnittstellen einrichten

Wenn eine HA-Gruppe konfiguriert wird, ist bekannt, mit welchen Knoten ONTAP eine Verbindung herstellt und welches StorageGRID Netzwerk verwendet wird. Es ist ebenfalls bekannt, welche Werte für die Subnetz-CIDR, die Gateway-IP-Adresse und die virtuellen IP-Adressen (VIP) einzugeben sind.

Wenn Sie ein virtuelles LAN zur Trennung des FabricPool-Datenverkehrs verwenden, wurde die VLAN-Schnittstelle bereits konfiguriert. Siehe "[\\${post_edited_translations.segment}](#)".

Identitätsföderation und SSO konfigurieren

Wenn für Ihr StorageGRID System Identitätsverbund oder Single Sign-On (SSO) vorgesehen ist, sind diese Funktionen aktiviert. Es ist ebenfalls bekannt, welche Verbundgruppe Root-Zugriff für das Mandantenkonto erhält, das ONTAP verwendet. Siehe "[Identitätsföderation verwenden](#)" und "[Einmalanmeldung konfigurieren](#)".

Domainnamen beziehen und konfigurieren

- Es ist bekannt, welcher vollqualifizierte Domainname (FQDN) für StorageGRID zu verwenden ist. Domain Name Server (DNS)-Einträge ordnen diesen FQDN den virtuellen IP-Adressen (VIP) der HA-Gruppe zu, die mit dem Assistenten erstellt wird. Siehe "[DNS-Server konfigurieren](#)".
- Wenn Sie S3-Anfragen im virtuellen Hosting-Stil verwenden möchten, haben Sie "[konfigurierte S3 Endpoint-Domännennamen](#)". ONTAP verwendet standardmäßig URLs im Pfadstil, aber die Verwendung von Anfragen im virtuellen Hosting-Stil wird empfohlen.

Überprüfung der Anforderungen an Load Balancer und Sicherheitszertifikate

Wenn die Verwendung des StorageGRID Load Balancer vorgesehen ist, wurden die allgemeinen "[Überlegungen zum Lastausgleich](#)" überprüft. Die Zertifikate, die hochgeladen werden, oder die Werte, die zur Generierung eines Zertifikats benötigt werden, liegen vor.

Wenn ein externer (Drittanbieter-)Load-Balancer-Endpunkt verwendet werden soll, sind der vollqualifizierte Domainname (FQDN), der Port und das Zertifikat für diesen Load Balancer vorhanden.

ILM Storage-Pool-Konfiguration bestätigen

Wenn StorageGRID 11.6 oder eine frühere Version ursprünglich installiert wurde, ist der Speicherpool, den Sie verwenden werden, konfiguriert. In der Regel sollte für jeden StorageGRID Standort, der zur Speicherung von ONTAP Daten verwendet wird, ein eigener Speicherpool erstellt werden.



Diese Voraussetzung gilt nicht, wenn StorageGRID 11.7 oder 11.8 ursprünglich installiert wurde. Bei der Erstinstallation einer dieser Versionen werden Speicherpools für jeden Standort automatisch erstellt.

Beziehung zwischen ONTAP und der StorageGRID Cloud-Tier

Der FabricPool Assistent führt durch den Prozess der Erstellung einer einzelnen StorageGRID Cloud-Tier, die einen StorageGRID Mandanten, einen Satz Zugriffsschlüssel und einen StorageGRID Bucket umfasst. Diese StorageGRID Cloud-Tier kann mit einer oder mehreren ONTAP lokalen Tiers verbunden werden.

Die Anbindung einer einzelnen Cloud-Ebene an mehrere lokale Ebenen in einem Cluster gilt allgemein als Best Practice. Je nach Anforderungen kann es jedoch sinnvoll sein, mehr als einen Bucket oder sogar mehr als einen StorageGRID Mandanten für die lokalen Ebenen in einem einzelnen Cluster zu verwenden. Die Verwendung unterschiedlicher Buckets und Mandanten ermöglicht die Isolation von Daten und Datenzugriff zwischen ONTAP lokalen Ebenen, ist jedoch etwas komplexer in der Konfiguration und Verwaltung.

NetApp empfiehlt nicht, eine einzelne Cloud-Ebene an lokale Ebenen in mehreren Clustern anzuhängen.



Die besten Vorgehensweisen für die Verwendung von StorageGRID mit NetApp MetroCluster™ und FabricPool Mirror sind unter ["TR-4598: FabricPool Best Practices in ONTAP"](#) zu finden.

Optional: Für jede lokale Ebene kann ein anderer Bucket verwendet werden.

Um in einem ONTAP Cluster mehr als einen Bucket für die lokalen Ebenen zu verwenden, muss in ONTAP mehr als eine StorageGRID Cloud-Ebene hinzugefügt werden. Jede Cloud-Ebene verwendet dieselbe HA-Gruppe, denselben Load-Balancer-Endpunkt, denselben Mandanten und dieselben Zugriffsschlüssel, verwendet jedoch einen anderen Container (StorageGRID Bucket). Die folgenden allgemeinen Schritte sind zu beachten:

1. Im StorageGRID Grid Manager den FabricPool Setup-Assistenten für die erste Cloud-Ebene ausführen.
2. Im ONTAP System Manager eine Cloud-Ebene hinzufügen und die von StorageGRID heruntergeladene Datei verwenden, um die erforderlichen Werte bereitzustellen.
3. Im StorageGRID Tenant Manager beim vom Assistenten erstellten Tenant anmelden und einen zweiten Bucket erstellen.
4. Den FabricPool Assistenten erneut abschließen. Die bestehende HA Gruppe, den Load Balancer Endpunkt und den Mandanten auswählen. Anschließend den neu erstellten Bucket auswählen. Eine neue ILM Regel für den neuen Bucket erstellen und eine ILM Richtlinie aktivieren, die diese Regel enthält.
5. In ONTAP eine zweite Cloud-Ebene hinzufügen, dabei den neuen Bucket-Namen angeben.

Optional: Für jede lokale Ebene kann ein anderer Mandant und Bucket verwendet werden.

Um in einem ONTAP Cluster mehr als einen Mandanten und unterschiedliche Zugriffsschlüssel für die lokalen Ebenen zu verwenden, wird in ONTAP mehr als eine StorageGRID Cloud-Ebene hinzugefügt. Jede Cloud-Ebene verwendet dieselbe HA-Gruppe und denselben Load-Balancer-Endpunkt, nutzt jedoch jeweils einen anderen Mandanten, andere Zugriffsschlüssel und einen anderen Container (StorageGRID Bucket). Dabei sind folgende allgemeine Schritte zu beachten:

1. Im StorageGRID Grid Manager den FabricPool Setup-Assistenten für die erste Cloud-Ebene ausführen.
2. Im ONTAP System Manager eine Cloud-Ebene hinzufügen und die von StorageGRID heruntergeladene Datei verwenden, um die erforderlichen Werte bereitzustellen.
3. Der FabricPool Assistent ist erneut auszuführen. Die vorhandene HA Gruppe und der Load Balancer Endpunkt sind auszuwählen. Ein neuer Mandant und ein neuer Bucket sind zu erstellen. Für den neuen Bucket ist eine neue ILM Regel zu erstellen und eine ILM Richtlinie zu aktivieren, die diese Regel einschließt.
4. In ONTAP eine zweite Cloud-Ebene hinzufügen, dabei den neuen Zugriffsschlüssel, den geheimen Schlüssel und den Bucket-Namen angeben.

Greifen Sie auf den StorageGRID FabricPool Einrichtungsassistenten zu und schließen Sie ihn ab

Sie können den FabricPool Setup-Assistenten verwenden, um StorageGRID als Objektspeichersystem für eine FabricPool Cloud-Tier zu konfigurieren.

Bevor Sie beginnen

- Sie haben die ["Überlegungen und Anforderungen"](#) Anleitung zur Verwendung des FabricPool Setup-Assistenten überprüft.



Wenn Sie StorageGRID für die Verwendung mit einer anderen S3-Clientanwendung konfigurieren möchten, gehen Sie zu "[S3-Einrichtungsassistent verwenden](#)".

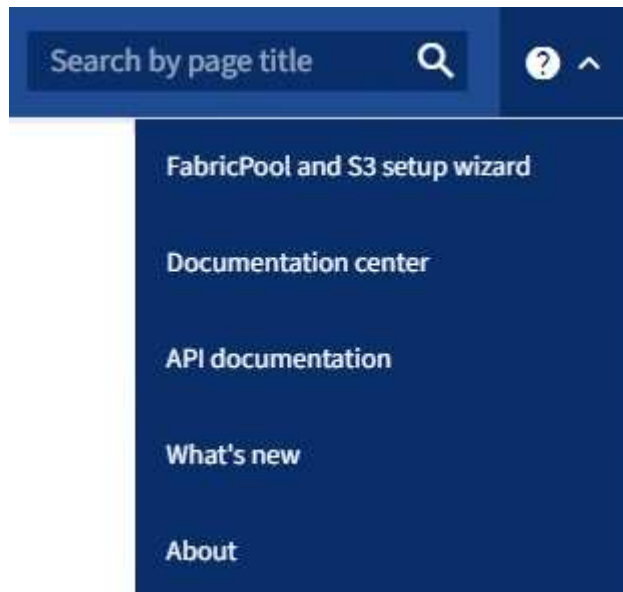
- Sie haben die "[Root-Zugriffsberechtigung](#)".

Assistenten aufrufen

Der FabricPool Einrichtungsassistent kann beim ersten Einsatz des StorageGRID Grid Managers abgeschlossen werden oder zu einem späteren Zeitpunkt aufgerufen und abgeschlossen werden.

Schritte

1. Melden Sie sich beim Grid Manager mit einem "[unterstützte Webbrowser](#)" an.
2. Wenn das Banner **FabricPool and S3 setup wizard** im Dashboard angezeigt wird, kann der Link im Banner ausgewählt werden. Wenn das Banner nicht mehr angezeigt wird, steht im Grid Manager das Hilfesymbol in der Kopfzeile zur Verfügung, über das **FabricPool and S3 setup wizard** ausgewählt werden kann.



3. Im FabricPool-Abschnitt der FabricPool und S3-Setup-Assistenten-Seite **Jetzt konfigurieren** auswählen.

Schritt 1 von 9: HA-Gruppe konfigurieren erscheint.

Schritt 1 von 9: HA-Gruppe konfigurieren

Eine Hochverfügbarkeitsgruppe (HA-Gruppe) ist eine Sammlung von Knoten, die jeweils den StorageGRID Load Balancer Service enthalten. Eine HA-Gruppe kann Gateway Nodes, Admin Nodes oder beides enthalten.

Eine HA-Gruppe kann dazu beitragen, FabricPool-Datenverbindungen verfügbar zu halten. Eine HA-Gruppe verwendet virtuelle IP-Adressen (VIPs), um hochverfügbaren Zugriff auf den Load Balancer-Service bereitzustellen. Fällt die aktive Schnittstelle in der HA-Gruppe aus, kann eine Backup-Schnittstelle die Arbeitslast mit minimalen Auswirkungen auf die FabricPool-Betriebsabläufe übernehmen.

Weitere Informationen zu dieser Aufgabe finden Sie unter "[Hochverfügbarkeitsgruppen verwalten](#)" und "[Bewährte Verfahren für Hochverfügbarkeitsgruppen](#)".

Schritte

1. Wenn Sie einen externen Load Balancer verwenden möchten, müssen Sie keine HA-Gruppe erstellen. **Diesen Schritt überspringen** auswählen und zu [Schritt 2 von 9: Load Balancer Endpunkt konfigurieren](#) gehen.
2. Für die Nutzung des StorageGRID Load Balancer wird eine neue HA-Gruppe erstellt oder eine vorhandene HA-Gruppe verwendet.

HA-Gruppe erstellen

- Zum Erstellen einer neuen HA-Gruppe **HA-Gruppe erstellen** auswählen.
- Für den Schritt **Details eingeben** sind die folgenden Felder auszufüllen.

Feld	Beschreibung
HA Gruppenname	Ein eindeutiger Anzeigename für diese HA Gruppe.
Beschreibung (optional)	Die Beschreibung dieser HA-Gruppe.

- Im Schritt **Schnittstellen hinzufügen** werden die Knotenschnittstellen ausgewählt, die in dieser HA-Gruppe verwendet werden sollen.

Mit den Spaltenüberschriften lassen sich die Zeilen sortieren, oder durch Eingabe eines Suchbegriffs können Schnittstellen schneller gefunden werden.

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

Die erste Schnittstelle in der Liste ist die Primary-Schnittstelle. Die Primary-Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.

Wenn die HA-Gruppe mehr als eine Schnittstelle umfasst und die aktive Schnittstelle ausfällt, werden die virtuellen IP-Adressen (VIP-Adressen) auf die erste Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. Fällt auch diese Schnittstelle aus, werden die VIP-Adressen auf die nächste Backup-Schnittstelle verschoben und so weiter. Wenn die Fehler behoben sind, wechseln die VIP-Adressen zurück auf die Schnittstelle mit der höchsten verfügbaren Priorität.

- Für den Schritt **IP-Adressen eingeben** sind die folgenden Felder auszufüllen.

Feld	Beschreibung
Subnetz CIDR	Die Adresse des VIP-Subnetzes in CIDR-Notation, eine IPv4-Adresse, gefolgt von einem Schrägstrich und der Subnetzlänge (0-32). Die Netzwerkadresse darf keine gesetzten Host-Bits aufweisen. Zum Beispiel 192.16.0.0/22.
Gateway-IP-Adresse (optional)	Optional. Wenn sich die für den Zugriff auf StorageGRID verwendeten ONTAP IP-Adressen nicht im selben Subnetz wie die StorageGRID VIP-Adressen befinden, geben Sie die IP-Adresse des lokalen Gateways der StorageGRID VIP ein. Die IP-Adresse des lokalen Gateways muss sich innerhalb des VIP-Subnetzes befinden.

Feld	Beschreibung
Virtuelle IP-Adresse	Geben Sie mindestens eine und höchstens zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden und sind gleichzeitig auf der aktiven Schnittstelle aktiv. Mindestens eine Adresse muss IPv4 sein. Optional können Sie zusätzliche IPv4- und IPv6-Adressen angeben.

f. **HA-Gruppe erstellen** auswählen und dann **Fertigstellen** auswählen, um zum FabricPool Setup-Assistenten zurückzukehren.

g. **Weiter** auswählen, um zum Load Balancer Schritt zu gelangen.

Vorhandene HA-Gruppe verwenden

a. Um eine bestehende HA-Gruppe zu verwenden, den Namen der HA-Gruppe aus der Dropdown-Liste **HA-Gruppe auswählen** auswählen.

b. **Weiter** auswählen, um zum Load Balancer Schritt zu gelangen.

Schritt 2 von 9: Load Balancer Endpunkt konfigurieren

StorageGRID verwendet einen Load Balancer, um die Arbeitslast von Clientanwendungen wie FabricPool zu verwalten. Durch Lastverteilung werden Geschwindigkeit und Verbindungskapazität über mehrere Storage Nodes hinweg maximiert.

Sie können den StorageGRID Load Balancer Service verwenden, der auf allen Gateway und Admin Nodes verfügbar ist, oder eine Verbindung zu einem externen (Drittanbieter) Load Balancer herstellen. Die Verwendung des StorageGRID Load Balancer wird empfohlen.

Weitere Informationen zu dieser Aufgabe finden sich in den allgemeinen ["Überlegungen zum Lastausgleich"](#) und den ["Best Practices für den Lastausgleich für FabricPool"](#).

Schritte

1. Wählen Sie einen StorageGRID Load Balancer Endpunkt aus oder erstellen Sie einen solchen, oder verwenden Sie einen externen Load Balancer.

`${post_edited_translations.segment}`

- a. **Endpunkt erstellen** auswählen.
- b. Für den Schritt **Endpunktdetails eingeben** sind die folgenden Felder auszufüllen.

Feld	Beschreibung
Name	<code>\${post_edited_translations.segment}</code>
Port	Der StorageGRID Port, den Sie für die Lastverteilung verwenden möchten. Dieses Feld ist standardmäßig auf 10433 für den ersten von Ihnen erstellten Endpunkt voreingestellt, Sie können jedoch jeden ungenutzten externen Port eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Nodes konfiguriert, da diese Ports auf Admin-Nodes reserviert sind. Hinweis: Die Nutzung von Ports, die von anderen Grid-Diensten verwendet werden, ist nicht zulässig. Siehe "Netzwerkport-Referenz".
Clienttyp	Muss S3 sein.
Netzwerkprotokoll	Wählen Sie HTTPS. Hinweis: Die Kommunikation mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen.

- c. Geben Sie für den Schritt **Bindungsmodus auswählen** den Bindungsmodus an. Der Bindungsmodus steuert, wie auf den Endpunkt über eine beliebige IP-Adresse oder über bestimmte IP-Adressen und Netzwerkschnittstellen zugegriffen wird.

Modus	Beschreibung
Global (Standard)	Clients können mit der IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, der virtuellen IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einem entsprechenden FQDN auf den Endpunkt zugreifen. Die Einstellung Global (Standard) sollte verwendet werden, es sei denn, die Zugänglichkeit dieses Endpunkts muss eingeschränkt werden.
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder den entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle die gleiche Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überschneiden.

Modus	Beschreibung
Knotenschnittstellen	Clients müssen die IP-Adressen (oder die entsprechenden FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Knotentyp	<code>\${post_edited_translations.segment}</code>

d. Für den Schritt **Mandantenzugriff** eine der folgenden Optionen auswählen:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen. Alle Mandanten zulassen ist fast immer die richtige Option für den Load-Balancer-Endpunkt, der für FabricPool verwendet wird. Diese Option ist auszuwählen, wenn der FabricPool Setup-Assistent für ein neues StorageGRID System verwendet wird und noch keine Mandantenkonten erstellt wurden.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Alle anderen Mandanten können diesen Endpunkt verwenden.

e. Für den Schritt **Zertifikat anhängen** eine der folgenden Optionen auswählen:

Feld	Beschreibung
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
Zertifikat generieren	Mit dieser Option kann ein selbstsigniertes Zertifikat generiert werden. Siehe " Load Balancer-Endpunkte konfigurieren " für Details zu den einzugebenden Informationen.
StorageGRID S3-Zertifikat verwenden	Diese Option ist nur verfügbar, wenn Sie bereits eine benutzerdefinierte Version des StorageGRID globalen Zertifikats hochgeladen oder generiert haben. Siehe " S3 API-Zertifikate konfigurieren " für Details.

f. **Fertigstellen** auswählen, um zum FabricPool Setup-Assistenten zurückzukehren.

g. `${post_edited_translations.segment}`



Änderungen an einem Endpunktzertifikat können bis zu 15 Minuten benötigen, um auf alle Knoten angewendet zu werden.

`${post_edited_translations.segment}`

- a. Wählen Sie den Namen eines vorhandenen Endpunkts aus der Dropdown-Liste **Select a load balancer endpoint** aus.
- b. `${post_edited_translations.segment}`

Externen Load Balancer verwenden

- a. Die folgenden Felder für den externen Load Balancer sind auszufüllen.

Feld	Beschreibung
FQDN	Der vollqualifizierte Domainname (FQDN) des externen Load Balancers.
Port	Die Portnummer, die FabricPool für die Verbindung zum externen Load Balancer verwendet.
Zertifikat	<code>\${post_edited_translations.segment}</code>

- b. `${post_edited_translations.segment}`

Schritt 3 von 9: Mandant und Bucket

Ein Mandant ist eine Entität, die S3-Anwendungen zum Speichern und Abrufen von Objekten in StorageGRID verwenden kann. Jeder Mandant verfügt über eigene Benutzer, Zugriffsschlüssel, Buckets, Objekte und einen spezifischen Satz an Funktionen. Ein StorageGRID Mandant muss erstellt werden, bevor der Bucket erstellt werden kann, den FabricPool verwendet.

Ein Bucket ist ein Container, der die Objekte und Objektmetadaten eines Mandanten speichert. Obwohl manche Mandanten mehrere Buckets haben können, ermöglicht der Assistent das Erstellen oder Auswählen jeweils nur eines Mandanten und eines Buckets. Mit dem Tenant Manager können später alle zusätzlichen benötigten Buckets hinzugefügt werden.

Sie können einen neuen Mandanten und Bucket für FabricPool verwenden erstellen oder einen bestehenden Mandanten und Bucket auswählen. Wenn ein neuer Mandant erstellt wird, generiert das System automatisch die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den Root-Benutzer.

Weitere Informationen zu dieser Aufgabe finden Sie unter ["Ein Mandantenkonto für FabricPool erstellen"](#) und ["Einen S3-Bucket erstellen und einen Zugriffsschlüssel erhalten"](#).

Schritte

Einen neuen Mandanten und Bucket erstellen oder einen bestehenden Mandanten auswählen.

Neuer Mandant und Bucket

1. Um einen neuen Mandanten und Bucket zu erstellen, einen **Mandantennamen** eingeben. Zum Beispiel `FabricPool tenant`.
2. Root-Zugriff für das Mandantenkonto definieren, abhängig davon, ob Ihr StorageGRID System "Identitätsföderation", "`{post_edited_translations.segment}`" oder beide verwendet.

Option	Tun Sie Folgendes
Wenn die Identitätsföderation nicht aktiviert ist	Das Passwort, das beim Anmelden beim Mandanten als lokaler Root-Benutzer verwendet wird, angeben.
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine vorhandene Verbundgruppe aus, die die Root-Zugriffsberechtigung für den Mandanten erhält. b. Optional kann das Passwort angegeben werden, das beim Anmelden beim Mandanten als lokaler Root-Benutzer verwendet wird.
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, der Root-Zugriff für den Mandanten gewährt wird. Lokale Benutzer können sich nicht anmelden.

3. Für **Bucket-Name** den Namen des Buckets eingeben, den FabricPool zum Speichern von ONTAP Daten verwendet. Zum Beispiel `fabricpool-bucket`.



Der Bucket-Name kann nach der Erstellung nicht mehr geändert werden.

4. Die **Region** für diesen Bucket auswählen.

Die Standardregion (`us-east-1`) sollte verwendet werden, es sei denn, es ist geplant, ILM zukünftig zum Filtern von Objekten basierend auf der Region des Buckets einzusetzen.

5. **Erstellen und fortfahren** auswählen, um den Mandanten und den Bucket zu erstellen und zum Schritt „Daten herunterladen“ zu gelangen

Mandant und Bucket auswählen

Das bestehende Mandantenkonto muss mindestens einen Bucket enthalten, für den keine Versionierung aktiviert ist. Ein bestehendes Mandantenkonto kann nicht ausgewählt werden, wenn für diesen Mandanten kein Bucket existiert.

1. Den bestehenden Mandanten aus der Dropdown-Liste **Tenant name** auswählen.
2. Den vorhandenen Bucket aus der Dropdown-Liste **Bucket name** auswählen.

FabricPool unterstützt keine Objektversionierung, daher werden Buckets, für die die Versionierung aktiviert ist, nicht angezeigt.



Wählen Sie keinen Bucket aus, bei dem S3 Object Lock für die Verwendung mit FabricPool aktiviert ist.

3. **Weiter** auswählen, um zum Schritt „Daten herunterladen“ zu gelangen.

Schritt 4 von 9: ONTAP-Einstellungen herunterladen

In diesem Schritt wird eine Datei heruntergeladen, mit der Werte in ONTAP System Manager eingegeben werden können.

Schritte

1. Optional kann das Kopiersymbol () ausgewählt werden, um sowohl die Zugriffsschlüssel-ID als auch den geheimen Zugriffsschlüssel in die Zwischenablage zu kopieren.

Diese Werte sind in der Download-Datei enthalten, aber möglicherweise möchten Sie sie separat speichern.

2. **ONTAP-Einstellungen herunterladen** auswählen, um eine Textdatei herunterzuladen, die die bisher eingegebenen Werte enthält.

Die `ONTAP_FabricPool_settings_bucketname.txt` Datei enthält die Informationen, die Sie benötigen, um StorageGRID als Objektspeichersystem für eine FabricPool Cloud-Ebene zu konfigurieren, einschließlich:

- Details zur Load Balancer-Verbindung, einschließlich Servername (FQDN), Port und Zertifikat
- Bucket Name
- Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel für den Root-Benutzer des Mandantenkontos

3. Die kopierten Schlüssel und die heruntergeladene Datei sollten an einem sicheren Ort aufbewahrt werden.



Schließen Sie diese Seite nicht, bevor Sie beide Zugriffsschlüssel kopiert, die ONTAP-Einstellungen heruntergeladen oder beides erledigt haben. Die Schlüssel sind nach dem Schließen dieser Seite nicht mehr verfügbar. Diese Informationen sollten an einem sicheren Ort aufbewahrt werden, da sie zum Abrufen von Daten aus Ihrem StorageGRID System verwendet werden können.

4. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel heruntergeladen oder kopiert wurden.
5. **Weiter** auswählen, um zum Schritt „ILM-Speicherpool“ zu gelangen.

Schritt 5 von 9: Auswahl eines Speicherpools

Ein Speicherpool ist eine Gruppe von Speicherknoten. Mit der Auswahl eines Speicherpools wird festgelegt, welche Knoten StorageGRID zum Speichern der von ONTAP ausgelagerten Daten verwendet.

Nähere Informationen zu diesem Schritt finden sich unter ["Einen Speicherpool erstellen"](#).

Schritte

1. In der Dropdown-Liste **Site** den StorageGRID Standort auswählen, der für die von ONTAP gestuften Daten verwendet werden soll.
2. In der Dropdown-Liste **Speicherpool** den Speicherpool für diesen Standort auswählen.

Der Speicherpool eines Standorts umfasst alle Storage Nodes an diesem Standort.

3. Wählen Sie **Weiter**, um zum ILM-Regelschritt zu gelangen.

Schritt 6 von 9: ILM-Regel für FabricPool überprüfen

Die Regeln des Information Lifecycle Management (ILM) steuern die Platzierung, die Dauer und das Aufnahmeverhalten aller Objekte in Ihrem StorageGRID System.

Der FabricPool Setup-Assistent erstellt automatisch die empfohlene ILM-Regel für die Verwendung mit FabricPool. Diese Regel gilt nur für den angegebenen Bucket. Es wird 2+1-Erasure-Coding an einem einzelnen Standort verwendet, um die von ONTAP ausgelagerten Daten zu speichern.

Nähere Informationen zu diesem Schritt finden Sie unter "[\\${post_edited_translations.segment}](#)" und "[Bewährte Verfahren für die Verwendung von ILM mit FabricPool Daten](#)".

Schritte

1. Die Regeldetails werden angezeigt.

Feld	Beschreibung
Regelname	Automatisch generiert und kann nicht geändert werden
Beschreibung	Automatisch generiert und kann nicht geändert werden
Filter	Der Bucket Name Diese Regel gilt nur für Objekte, die in dem von Ihnen angegebenen Bucket gespeichert sind.
Referenzzeit	Ingest-Zeitpunkt Die Platzierungsanweisung beginnt, sobald Objekte zum ersten Mal im Bucket gespeichert werden.
Platzierungsanweisung	2+1-Löschcodierung

2. Das Aufbewahrungsdigramm nach **Zeitraum** und **Speicherpool** sortieren, um die Platzierungsanweisung zu bestätigen.
 - Der **Zeitraum** für die Regel ist **Tag 0 - unbegrenzt**. **Tag 0** bedeutet, dass die Regel angewendet wird, wenn Daten von ONTAP gestuft werden. **Unbegrenzt** bedeutet, dass StorageGRID ILM keine Daten löscht, die von ONTAP gestuft wurden.
 - Der **Storage pool** für die Regel ist der von Ihnen ausgewählte Storage pool. **EC 2+1** bedeutet, dass die Daten mit 2+1-Erasure-Coding gespeichert werden. Jedes Objekt wird als zwei Datenfragmente und ein Paritätsfragment gespeichert. Die drei Fragmente jedes Objekts werden auf unterschiedlichen Storage Nodes an einem einzigen Standort gespeichert.
3. **Erstellen und Fortfahren** auswählen, um diese Regel zu erstellen und zum ILM-Richtlinienschritt zu wechseln.

Schritt 7 von 9: ILM-Richtlinie prüfen und aktivieren

Nachdem der FabricPool Setup-Assistent die ILM-Regel für die Verwendung mit FabricPool erstellt hat, wird eine ILM-Richtlinie erstellt. Diese Richtlinie muss vor der Aktivierung sorgfältig simuliert und überprüft werden.

Nähere Informationen zu diesem Schritt finden Sie unter "[ILM-Richtlinie erstellen](#)" und "[Bewährte Verfahren für die Verwendung von ILM mit FabricPool Daten](#)".



Wenn eine neue ILM-Richtlinie aktiviert wird, verwendet StorageGRID diese Richtlinie, um die Platzierung, Dauer und den Datenschutz aller Objekte im Grid zu verwalten, einschließlich bestehender und neu hinzugefügter Objekte. In einigen Fällen kann die Aktivierung einer neuen Richtlinie dazu führen, dass bestehende Objekte an neue Speicherorte verschoben werden.



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

Schritte

1. Optional können Sie den vom System generierten **Richtliniennamen** aktualisieren. Standardmäßig hängt das System „+ FabricPool“ an den Namen Ihrer aktiven oder inaktiven Richtlinie an, aber Sie können auch einen eigenen Namen angeben.
2. Die Liste der Regeln in der inaktiven Richtlinie kann überprüft werden.
 - Falls Ihr Grid keine inaktive ILM-Richtlinie besitzt, erstellt der Assistent eine inaktive Richtlinie, indem er Ihre aktive Richtlinie klonet und die neue Regel oben hinzufügt.
 - Wenn Ihr Grid bereits über eine inaktive ILM-Richtlinie verfügt und diese Richtlinie dieselben Regeln und dieselbe Reihenfolge wie die aktive ILM-Richtlinie verwendet, fügt der Assistent die neue Regel oben in die inaktive Richtlinie ein.
 - Wenn Ihre inaktive Richtlinie andere Regeln oder eine andere Reihenfolge als die aktive Richtlinie enthält, erstellt der Assistent eine neue inaktive Richtlinie, indem er Ihre aktive Richtlinie klonet und die neue Regel oben hinzufügt.
3. Die Reihenfolge der Regeln in der neuen inaktiven Richtlinie sollte überprüft werden.

Da die FabricPool-Regel die erste Regel ist, werden alle Objekte im FabricPool-Bucket platziert, bevor die anderen Regeln der Richtlinie ausgewertet werden. Objekte in allen anderen Buckets werden durch nachfolgende Regeln der Richtlinie platziert.

4. Im Retentionsdiagramm wird dargestellt, wie verschiedene Objekte aufbewahrt werden.
 - a. **Alle erweitern** zeigt ein Aufbewahrungsdigramm für jede Regel in der inaktiven Richtlinie.
 - b. Wählen Sie **Zeitraum** und **Speicherpool** aus, um das Aufbewahrungsdigramm anzuzeigen. Bestätigen Sie, dass alle Regeln, die für den FabricPool Bucket oder Mandanten gelten, Objekte **für immer** aufbewahren.
5. Nachdem Sie die inaktive Richtlinie überprüft haben, **Aktivieren und fortfahren** auswählen, um die Richtlinie zu aktivieren und zum Schritt der Verkehrsklassifizierung zu gelangen.



Fehler in einer ILM-Richtlinie können zu irreparabilem Datenverlust führen. Die Richtlinie sollte sorgfältig geprüft werden, bevor sie aktiviert wird.

Schritt 8 von 9: Verkehrsklassifizierungsrichtlinie erstellen

Optional kann der FabricPool Einrichtungsassistent eine Richtlinie zur Datenverkehrsklassifizierung erstellen, mit der die FabricPool Arbeitslast überwacht werden kann. Die vom System erstellte Richtlinie verwendet eine Abgleichsregel, um den gesamten Netzwerkverkehr zu identifizieren, der mit dem von Ihnen erstellten Bucket verknüpft ist. Diese Richtlinie überwacht ausschließlich den Datenverkehr; sie beschränkt den Datenverkehr weder für FabricPool noch für andere Clients.

Nähere Informationen zu diesem Schritt finden sich unter ["Eine Verkehrsklassifizierungsrichtlinie für FabricPool erstellen"](#).

Schritte

1. Die Richtlinie wird überprüft.
2. Wenn diese Richtlinie zur Verkehrsklassifizierung erstellt werden soll, **Erstellen und fortfahren** auswählen.

Sobald FabricPool mit dem Tiering von Daten zu StorageGRID beginnt, kann auf der Seite „Traffic Classification Policies“ die Netzwerkverkehrsmetriken für diese Richtlinie angezeigt werden. Später können auch Regeln hinzugefügt werden, um andere Workloads zu begrenzen und sicherzustellen, dass der FabricPool Workload den Großteil der Bandbreite erhält.

3. Andernfalls **Diesen Schritt überspringen** auswählen.

Schritt 9 von 9: Zusammenfassung überprüfen

Die Zusammenfassung enthält Details zu den von Ihnen konfigurierten Elementen, einschließlich des Namens des Load Balancers, des Mandanten und des Buckets, der Richtlinie zur Datenverkehrsklassifizierung und der aktiven ILM-Richtlinie,

Schritte

1. Überprüfen Sie die Zusammenfassung.
2. Wählen Sie **Fertigstellen**.

Nächste Schritte

Nach Abschluss des FabricPool Assistenten sind diese zusätzlichen Schritte durchzuführen.

Schritte

1. Wechseln Sie zu ["ONTAP System Manager konfigurieren"](#), um die gespeicherten Werte einzugeben und die ONTAP-Seite der Verbindung abzuschließen. StorageGRID muss als Cloud-Tier hinzugefügt, das Cloud-Tier mit einem lokalen Tier verbunden werden, um eine FabricPool zu erstellen, und Volume-Tiering-Richtlinien müssen festgelegt werden.
2. Wechseln Sie zu ["Den DNS-Server konfigurieren"](#) und stellen Sie sicher, dass der DNS einen Eintrag enthält, der den StorageGRID Servernamen (vollqualifizierte Domain) mit jeder StorageGRID IP-Adresse verknüpft, die verwendet wird.
3. Informationen zu Best Practices für StorageGRID Audit-Logs und weitere globale Konfigurationsoptionen finden sich unter ["Weitere Best Practices für StorageGRID und FabricPool"](#).

StorageGRID manuell konfigurieren

Erstellen Sie eine Hochverfügbarkeitsgruppe (HA) für FabricPool in StorageGRID

Bei der Konfiguration von StorageGRID für die Verwendung mit FabricPool können optional eine oder mehrere hochverfügbare Gruppen (HA-Gruppen) erstellt werden. Eine HA-Gruppe ist eine Sammlung von Knoten, die jeweils den StorageGRID Load Balancer Service enthalten. Eine HA-Gruppe kann Gateway Nodes, Admin Nodes oder beide enthalten.

Eine HA-Gruppe kann verwendet werden, um FabricPool-Datenverbindungen verfügbar zu halten. Eine HA-Gruppe verwendet virtuelle IP-Adressen (VIPs), um hochverfügbaren Zugriff auf den Load Balancer-Service bereitzustellen. Fällt die aktive Schnittstelle in der HA-Gruppe aus, kann eine Backup-Schnittstelle die Arbeitslast mit minimalen Auswirkungen auf die FabricPool-Betriebsabläufe übernehmen.

Weitere Informationen zu dieser Aufgabe finden sich unter ["Hochverfügbarkeitsgruppen verwalten"](#). Zur Ausführung dieser Aufgabe mit dem FabricPool Setup-Assistenten kann ["Den FabricPool Setup-Assistenten aufrufen und abschließen"](#) aufgerufen werden.

Bevor Sie beginnen

- Sie haben die ["Best Practices für hochverfügbare Gruppen"](#) überprüft.
- Sie sind mit einem ["unterstützte Webbrowser"](#) beim Grid Manager angemeldet.
- Sie haben die ["Root-Zugriffsberechtigung"](#).
- Wenn Sie ein VLAN verwenden möchten, haben Sie die VLAN-Schnittstelle erstellt. Siehe ["\\${post_edited_translations.segment}"](#).

Schritte

1. **Konfiguration > Netzwerk > Hochverfügbarkeitsgruppen** auswählen.
2. Wählen Sie **Create**.
3. Für den Schritt **Details eingeben** sind die folgenden Felder auszufüllen.

Feld	Beschreibung
HA Gruppenname	Ein eindeutiger Anzeigenname für diese HA Gruppe.
Beschreibung (optional)	Die Beschreibung dieser HA-Gruppe.

4. Im Schritt **Schnittstellen hinzufügen** werden die Knotenschnittstellen ausgewählt, die in dieser HA-Gruppe verwendet werden sollen.

Mit den Spaltenüberschriften lassen sich die Zeilen sortieren, oder durch Eingabe eines Suchbegriffs können Schnittstellen schneller gefunden werden.

[\\${post_edited_translations.segment}](#)

5. [\\${post_edited_translations.segment}](#)

[\\${post_edited_translations.segment}](#)

Die erste Schnittstelle in der Liste ist die Primary-Schnittstelle. Die Primary-Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.

Wenn die HA-Gruppe mehr als eine Schnittstelle umfasst und die aktive Schnittstelle ausfällt, werden die virtuellen IP-Adressen (VIP-Adressen) auf die erste Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. Fällt auch diese Schnittstelle aus, werden die VIP-Adressen auf die nächste Backup-Schnittstelle verschoben und so weiter. Wenn die Fehler behoben sind, wechseln die VIP-Adressen zurück auf die Schnittstelle mit der höchsten verfügbaren Priorität.

6. Für den Schritt **IP-Adressen eingeben** sind die folgenden Felder auszufüllen.

Feld	Beschreibung
Subnetz CIDR	Die Adresse des VIP-Subnetzes in CIDR-Notation, eine IPv4-Adresse, gefolgt von einem Schrägstrich und der Subnetzlänge (0-32). Die Netzwerkadresse darf keine gesetzten Host-Bits aufweisen. Zum Beispiel 192.16.0.0/22.
Gateway-IP-Adresse (optional)	Optional. Wenn sich die für den Zugriff auf StorageGRID verwendeten ONTAP IP-Adressen nicht im selben Subnetz wie die StorageGRID VIP-Adressen befinden, geben Sie die IP-Adresse des lokalen Gateways der StorageGRID VIP ein. Die IP-Adresse des lokalen Gateways muss sich innerhalb des VIP-Subnetzes befinden.
Virtuelle IP-Adresse	Geben Sie mindestens eine und höchstens zehn VIP-Adressen für die aktive Schnittstelle in der HA Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden. Mindestens eine Adresse muss IPv4 sein. Optional können Sie zusätzliche IPv4- und IPv6-Adressen angeben.

7. **HA-Gruppe erstellen** auswählen und dann **Fertigstellen** wählen.

Erstellen Sie einen Load-Balancer-Endpunkt für FabricPool in StorageGRID

StorageGRID verwendet einen Load Balancer, um die Arbeitslast von Clientanwendungen wie FabricPool zu verwalten. Durch Lastverteilung werden Geschwindigkeit und Verbindungskapazität über mehrere Storage Nodes hinweg maximiert.

Bei der Konfiguration von StorageGRID für die Verwendung mit FabricPool muss ein Load-Balancer-Endpunkt konfiguriert und ein Load-Balancer-Endpunktzertifikat hochgeladen oder generiert werden, das zur Sicherung der Verbindung zwischen ONTAP und StorageGRID verwendet wird.

Um den FabricPool Einrichtungsassistenten für diese Aufgabe zu verwenden, gehen Sie zu ["Den FabricPool Setup-Assistenten aufrufen und abschließen"](#).

Bevor Sie beginnen

- Sie sind mit einem ["unterstützte Webbrowser"](#) beim Grid Manager angemeldet.
- Sie haben die ["Root-Zugriffsberechtigung"](#).
- Sie haben das allgemeine ["Überlegungen zum Lastausgleich"](#) sowie das ["Best Practices für den Lastausgleich für FabricPool"](#) überprüft.

Schritte

1. **Konfiguration > Netzwerk > Load balancer endpoints** auswählen.
2. Wählen Sie **Create**.
3. Für den Schritt **Endpunktdetails eingeben** sind die folgenden Felder auszufüllen.

Feld	Beschreibung
Name	<code>\${post_edited_translations.segment}</code>
Port	Der StorageGRID Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist für den ersten von Ihnen erstellten Endpunkt standardmäßig auf 10433 gesetzt, aber Sie können jeden ungenutzten externen Port eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway Nodes konfiguriert. Diese Ports sind auf Admin Nodes reserviert. Hinweis: Die Nutzung von Ports, die von anderen Grid-Diensten verwendet werden, ist nicht zulässig. Siehe "Netzwerkport-Referenz". Diese Nummer wird ONTAP bereitgestellt, wenn StorageGRID als FabricPool Cloud-Tier angebunden wird.
Clienttyp	S3 auswählen.
Netzwerkprotokoll	Wählen Sie HTTPS. Hinweis: Die Kommunikation mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen.

4. Geben Sie für den Schritt **Bindungsmodus auswählen** den Bindungsmodus an. Der Bindungsmodus steuert, wie auf den Endpunkt über eine beliebige IP-Adresse oder über bestimmte IP-Adressen und Netzwerkschnittstellen zugegriffen wird.

Modus	Beschreibung
Global (Standard)	Clients können mit der IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, der virtuellen IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einem entsprechenden FQDN auf den Endpunkt zugreifen. Die Einstellung Global (Standard) sollte verwendet werden, es sei denn, die Zugänglichkeit dieses Endpunkts muss eingeschränkt werden.
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder den entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle die gleiche Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überschneiden.
Knotenschnittstellen	Clients müssen die IP-Adressen (oder die entsprechenden FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Knotentyp	<code>\${post_edited_translations.segment}</code>

5. Für den Schritt **Mandantenzugriff** eine der folgenden Optionen auswählen:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen. Alle Mandanten zulassen ist fast immer die richtige Option für den Load-Balancer-Endpoint, der für FabricPool verwendet wird. Diese Option ist auszuwählen, wenn noch keine Mandantenkonten erstellt wurden.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Alle anderen Mandanten können diesen Endpunkt verwenden.

6. Für den Schritt **Zertifikat anhängen** eine der folgenden Optionen auswählen:

Feld	Beschreibung
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
Zertifikat generieren	Mit dieser Option kann ein selbstsigniertes Zertifikat generiert werden. Siehe " Load Balancer-Endpunkte konfigurieren " für Details zu den einzugebenden Informationen.
StorageGRID S3-Zertifikat verwenden	Diese Option ist nur verfügbar, wenn Sie bereits eine benutzerdefinierte Version des StorageGRID globalen Zertifikats hochgeladen oder generiert haben. Siehe " S3 API-Zertifikate konfigurieren " für Details.

7. Wählen Sie **Create**.



Änderungen an einem Endpunktzertifikat können bis zu 15 Minuten benötigen, um auf alle Knoten angewendet zu werden.

Erstellen Sie ein Mandantenkonto für FabricPool in StorageGRID

Im Grid Manager ist ein Mandantenkonto für die Nutzung von FabricPool zu erstellen.

Mandantenkonten ermöglichen es Clientanwendungen, Objekte auf StorageGRID zu speichern und abzurufen. Jedes Mandantenkonto verfügt über eine eigene Konto-ID, autorisierte Gruppen und Benutzer, Buckets und Objekte.

Weitere Informationen zu dieser Aufgabe finden sich unter "[Mandantenkonto erstellen](#)". Zur Verwendung des

FabricPool Setup-Assistenten für diese Aufgabe siehe ["Den FabricPool Setup-Assistenten aufrufen und abschließen"](#).

Bevor Sie beginnen

- Sie sind mit einem ["unterstützte Webbrowser"](#) beim Grid Manager angemeldet.
- Du hast ["spezifische Zugriffsberechtigungen"](#).

Schritte

1. **Tenants** auswählen.
2. Wählen Sie **Create**.
3. Für die Schritte „Details eingeben“ sind die folgenden Informationen anzugeben.

Feld	Beschreibung
Name	Ein Name für das Mandantenkonto. Mandantennamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, numerische Konto-ID.
Beschreibung (optional)	Eine Beschreibung zur Identifizierung des Tenants.
Clienttyp	Muss S3 für FabricPool sein.
Speicherkontingent (optional)	Dieses Feld für FabricPool leer lassen.

4. Für den Schritt „Berechtigungen auswählen“:

- a. **Plattformdienste zulassen** darf nicht ausgewählt werden.

FabricPool Mandanten benötigen in der Regel keine Plattformdienste wie die CloudMirror Replikation.

- b. Optional kann **Eigene Identitätsquelle verwenden** ausgewählt werden.

- c. **S3 Select zulassen** sollte nicht ausgewählt werden.

FabricPool Mandanten müssen S3 Select in der Regel nicht verwenden.

- d. Optional kann **Grid-Federationsverbindung verwenden** ausgewählt werden, um dem Mandanten die Verwendung eines ["Grid Federation Verbindung"](#) für Kontoklon und gridübergreifende Replikation zu ermöglichen. Anschließend wird die zu verwendende Grid-Federationsverbindung ausgewählt.

5. Geben Sie im Schritt „Root-Zugriff definieren“ an, welcher Benutzer die anfängliche Root-Zugriffsberechtigung für das Mandantenkonto erhält, abhängig davon, ob Ihr StorageGRID System ["Identitätsföderation"](#), ["\\${post_edited_translations.segment}"](#) oder beides verwendet.

Option	Tun Sie Folgendes
Wenn die Identitätsföderation nicht aktiviert ist	Das Passwort, das beim Anmelden beim Mandanten als lokaler Root-Benutzer verwendet wird, angeben.

Option	Tun Sie Folgendes
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine vorhandene Verbundgruppe aus, die die Root-Zugriffsberechtigung für den Mandanten erhält. b. Optional kann das Passwort angegeben werden, das beim Anmelden beim Mandanten als lokaler Root-Benutzer verwendet wird.
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, der Root-Zugriff für den Mandanten gewährt wird. Lokale Benutzer können sich nicht anmelden.

6. **Mandant erstellen** auswählen.

Erstellen Sie einen S3-Bucket und rufen Sie Zugriffsschlüssel für FabricPool in StorageGRID ab

Bevor StorageGRID mit einer FabricPool Arbeitslast verwendet wird, muss ein S3-Bucket für die FabricPool Daten erstellt werden. Außerdem werden ein Zugriffsschlüssel und ein geheimer Zugriffsschlüssel für das Mandantenkonto benötigt, das für FabricPool verwendet wird.

Weitere Informationen zu dieser Aufgabe finden sich unter ["S3 Bucket erstellen"](#) und ["Eigene S3-Zugriffsschlüssel erstellen"](#). Um den FabricPool Setup-Assistenten für diese Aufgabe zu verwenden, gehen Sie zu ["Den FabricPool Setup-Assistenten aufrufen und abschließen"](#).

Bevor Sie beginnen

- Sie haben ein Mandantenkonto für die FabricPool Nutzung erstellt.
- Sie haben Root-Zugriff auf das Mandantenkonto.

Schritte

1. Im Tenant Manager anmelden.

Es stehen folgende Optionen zur Verfügung:

- Auf der Seite „Mandantenkonten“ im Grid Manager wird der Link **Anmelden** für den Mandanten ausgewählt und die Zugangsdaten werden eingegeben.
- Geben Sie die URL des Mandantenkontos in einem Webbrowser ein und melden Sie sich mit Ihren Zugangsdaten an.

2. Einen S3-Bucket für FabricPool-Daten erstellen.

Für jeden ONTAP Cluster, der verwendet werden soll, ist ein eigener Bucket zu erstellen.

- View buckets** im Dashboard auswählen oder **STORAGE (S3) > Buckets**.
- Bucket erstellen** auswählen.
- Geben Sie den Namen des StorageGRID Buckets ein, den Sie mit FabricPool verwenden möchten. Zum Beispiel `fabricpool-bucket`.



Der Bucket-Name kann nach der Erstellung nicht mehr geändert werden.

- d. Wählen Sie die Region für diesen Bucket aus.

Standardmäßig werden alle Buckets in der `us-east-1` Region erstellt. Wenn als Standardregion eine andere Region als `us-east-1` konfiguriert ist, wird diese andere Region zunächst im Dropdown-Menü ausgewählt.

- e. Wählen Sie **Weiter**.

- f. **Bucket erstellen** auswählen.



Wählen Sie für den FabricPool Bucket nicht die Option **Objektversionierung aktivieren**. Ebenso sollte ein FabricPool Bucket nicht so bearbeitet werden, dass **Verfügbar** oder eine andere als die Standardkonsistenz verwendet wird. Die empfohlene Bucket-Konsistenz für FabricPool Buckets ist **Read-after-new-write**, was die Standardkonsistenz für einen neuen Bucket ist.

3. Ein Zugriffsschlüssel und ein geheimer Zugriffsschlüssel werden erstellt.

- a. **SPEICHER (S3) > Meine Zugriffsschlüssel** auswählen.

- b. **Schlüssel erstellen** auswählen.

- c. **Zugriffsschlüssel erstellen** auswählen.

- d. Die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel können an einem sicheren Ort gespeichert oder mit **Download .csv** als Tabellenkalkulationsdatei mit Zugriffsschlüssel-ID und geheimem Zugriffsschlüssel heruntergeladen werden.

Diese Werte werden in ONTAP eingegeben, wenn StorageGRID als FabricPool Cloud-Tier konfiguriert wird.



Wenn Sie in Zukunft einen neuen Zugriffsschlüssel und geheimen Zugriffsschlüssel in StorageGRID generieren, geben Sie die neuen Schlüssel in ONTAP ein, bevor Sie die alten Werte aus StorageGRID löschen. Andernfalls verliert ONTAP möglicherweise vorübergehend den Zugriff auf StorageGRID.

StorageGRID ILM für FabricPool-Daten konfigurieren

Diese einfache Beispielrichtlinie kann als Ausgangspunkt für eigene ILM-Regeln und Richtlinien dienen.

Dieses Beispiel geht davon aus, dass Sie die ILM-Regeln und eine ILM-Richtlinie für ein StorageGRID System mit vier Storage Nodes in einem einzigen Rechenzentrum in Denver, Colorado, entwerfen. Die FabricPool Daten in diesem Beispiel verwenden einen Bucket mit dem Namen `fabricpool-bucket`.



Die folgenden ILM-Regeln und die Richtlinie sind lediglich Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Vor der Aktivierung einer neuen Richtlinie sollte diese simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert und Inhalte vor Datenverlust schützt. Weitere Informationen finden sich unter "[Objekte mit ILM verwalten](#)".



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

Bevor Sie beginnen

- Sie haben die "[Best Practices für die Verwendung von ILM mit FabricPool Daten](#)" überprüft.
- Sie sind mit einem "[unterstützte Webbrowser](#)" beim Grid Manager angemeldet.
- Sie haben die "[ILM- oder Root-Zugriff-Berechtigung](#)".
- Wenn Sie StorageGRID von einer StorageGRID Version vor 11.7 auf 12.0 aktualisiert haben, haben Sie den Speicherpool, den Sie verwenden werden, bereits konfiguriert. Im Allgemeinen sollte für jeden StorageGRID Standort, den Sie zum Speichern von Daten verwenden, ein Speicherpool erstellt werden. (Ab Version 11.7 werden Speicherpools automatisch für jeden Standort erstellt.)



Diese Voraussetzung gilt nicht, wenn StorageGRID 11.7 oder 11.8 ursprünglich installiert wurde. Bei der Erstinstallation einer dieser Versionen werden Speicherpools für jeden Standort automatisch erstellt.

Schritte

1. Erstellen Sie eine ILM-Regel, die nur für die Daten in `fabricpool-bucket` gilt. Diese Beispielregel erstellt löschcodierte Kopien.

Regeldefinition	Beispielwert
Regelname	2 + 1 Löschcodierung für FabricPool Daten
Bucket Name	<code>fabricpool-bucket</code> Es besteht auch die Möglichkeit, nach dem FabricPool Mandantenkonto zu filtern.
Erweiterte Filter	Objektgröße größer als 0,2 MB. Hinweis: FabricPool schreibt nur 4 MB große Objekte, aber es ist erforderlich, einen Objektgrößenfilter hinzuzufügen, da diese Regel Erasure Coding verwendet.
Referenzzeit	Ingest-Zeitpunkt
Zeitraum und Platzierungen	Ab Tag 0 für immer speichern Objekte werden mittels Erasure Coding unter Verwendung des 2+1 EC-Schemas in Denver gespeichert und diese Objekte dauerhaft in StorageGRID aufbewahrt.  Um Datenverlust zu vermeiden, sollte keine ILM-Regel verwendet werden, die abläuft oder FabricPool Cloud-Tier-Daten löscht.

Regeldefinition	Beispielwert
Ingest-Verhalten	Ausgewogen

2. Eine Standard-ILM-Regel erstellen, die zwei replizierte Kopien aller Objekte erzeugt, die nicht von der ersten Regel erfasst werden. Keinen einfachen Filter (Mandantenkonto oder Bucket-Name) oder erweiterte Filter auswählen.

Regeldefinition	Beispielwert
Regelname	Zwei replizierte Kopien
Bucket Name	<i>none</i>
Erweiterte Filter	<i>none</i>
Referenzzeit	Ingest-Zeitpunkt
Zeitraum und Platzierungen	Ab Tag 0 für immer speichern Objekte werden gespeichert, indem zwei Kopien in Denver repliziert werden.
Ingest-Verhalten	Ausgewogen

3. Eine ILM-Richtlinie erstellen und die beiden Regeln auswählen. Da die Replikationsregel keine Filter verwendet, kann sie die Standardregel (letzte Regel) für die Richtlinie sein.
4. Testobjekte in das Grid einlesen.
5. Die Richtlinie kann mit den Testobjekten simuliert werden, um das Verhalten zu überprüfen.
6. Die Richtlinie wird aktiviert.

Wenn diese Richtlinie aktiviert ist, platziert StorageGRID Objektdaten wie folgt:

- Die von FabricPool in `fabricpool-bucket` gestaffelten Daten werden mit dem 2+1-Erasure-Coding-Schema erasure-codiert. Zwei Datenfragmente und ein Paritätsfragment werden auf drei verschiedenen Storage Nodes abgelegt.
- Alle Objekte in allen anderen Buckets werden repliziert. Zwei Kopien werden erstellt und auf zwei verschiedenen Storage Nodes abgelegt.
- Die Kopien bleiben in StorageGRID dauerhaft erhalten. StorageGRID ILM löscht diese Objekte nicht.

Erstellen Sie eine Richtlinie zur Verkehrsklassifizierung für FabricPool in StorageGRID

Optional kann eine StorageGRID Datenverkehrsklassifizierungsrichtlinie entworfen werden, um die Dienstqualität für die FabricPool Arbeitslast zu optimieren.

Weitere Informationen zu dieser Aufgabe finden sich unter ["Verkehrsklassifizierungsrichtlinien verwalten"](#). Zur Ausführung dieser Aufgabe mit dem FabricPool Setup-Assistenten siehe ["Den FabricPool Setup-Assistenten"](#)

aufrufen und abschließen".

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".

Über diese Aufgabe

Die besten Vorgehensweisen zur Erstellung einer Richtlinie zur Verkehrsklassifizierung für FabricPool hängen von der Arbeitslast ab, wie folgt:

- Wenn geplant ist, primäre FabricPool-Workload-Daten nach StorageGRID zu verschieben, sollte sichergestellt werden, dass der FabricPool-Workload den Großteil der Bandbreite erhält. Eine Richtlinie zur Datenverkehrsklassifizierung kann erstellt werden, um alle anderen Workloads zu begrenzen.



Im Allgemeinen ist es wichtiger, FabricPool-Leseoperationen zu priorisieren als Schreiboperationen.

Wenn beispielsweise andere S3-Clients dieses StorageGRID System nutzen, sollte eine Richtlinie zur Datenverkehrsklassifizierung erstellt werden. Der Netzwerkverkehr für die anderen Buckets, Mandanten, IP-Subnetze oder Load-Balancer-Endpunkte kann begrenzt werden.

- Generell sollten keine Qualitätsbeschränkungen für FabricPool Arbeitslasten festgelegt werden; nur die anderen Arbeitslasten sollten beschränkt werden.
- Die für andere Arbeitslasten festgelegten Beschränkungen sollten deren Verhalten berücksichtigen. Die festgelegten Beschränkungen variieren zudem je nach Dimensionierung und Leistungsfähigkeit Ihres Grids sowie der erwarteten Auslastung.

Schritte

1. **Konfiguration > Netzwerk > Verkehrsklassifizierung** auswählen.
2. Wählen Sie **Create**.
3. Geben Sie einen Namen und eine optionale Beschreibung für die Richtlinie ein und wählen Sie **Weiter**.
4. Im Schritt „Übereinstimmende Regeln hinzufügen“ wird mindestens eine Regel hinzugefügt.
 - a. **Regel hinzufügen** auswählen
 - b. Für Typ **Load balancer endpoint** auswählen und den Load balancer endpoint auswählen, der für FabricPool erstellt wurde.

Sie können auch das FabricPool Mandantenkonto oder den Bucket auswählen.

- c. Wenn diese Datenverkehrsrichtlinie den Datenverkehr für die anderen Endpunkte einschränken soll, ist **Umgekehrte Übereinstimmung** auszuwählen.
5. Optional lassen sich eine oder mehrere Beschränkungen hinzufügen, um den von der Regel erfassten Netzwerkverkehr zu steuern.



StorageGRID erfasst Metriken auch dann, wenn Sie keine Limits hinzufügen, sodass Sie die Verkehrstrends nachvollziehen können.

- a. **Limit hinzufügen** auswählen.
- b. Wählen Sie die Art des Datenverkehrs aus, den Sie begrenzen möchten, sowie das anzuwendende Limit.

6. Wählen Sie **Weiter**.

7. Die Richtlinie zur Verkehrsklassifizierung wird gelesen und geprüft. Mit der Schaltfläche **Zurück** besteht die Möglichkeit, bei Bedarf Änderungen vorzunehmen. Ist die Richtlinie zufriedenstellend, kann **Speichern und fortfahren** ausgewählt werden.

Nach Abschluss

["Netzwerkverkehrsmetriken"](#) um zu überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsbeschränkungen durchsetzen.

Konfigurieren Sie ONTAP System Manager, um StorageGRID als FabricPool Cloud-Tier hinzuzufügen

Nachdem Sie die erforderlichen StorageGRID Informationen erhalten haben, kann in ONTAP StorageGRID als Cloud-Tier hinzugefügt werden.

Bevor Sie beginnen

- Wenn Sie den FabricPool Einrichtungsassistenten vollständig durchlaufen haben, verfügen Sie über die `ONTAP_FabricPool_settings_bucketname.txt` Datei, die Sie heruntergeladen haben.
- Wenn StorageGRID manuell konfiguriert wurde, stehen der vollqualifizierte Domainname (FQDN), der für StorageGRID verwendet wird, oder die virtuelle IP-Adresse (VIP) für die StorageGRID HA-Gruppe, die Portnummer für den Load-Balancer-Endpunkt, das Load-Balancer-Zertifikat, die Access Key ID und der Secret Key für den Root-Benutzer des Mandantenkontos sowie der Name des Buckets, den ONTAP in diesem Mandanten verwendet, zur Verfügung.

Auf ONTAP System Manager zugreifen

Diese Anleitung beschreibt, wie ONTAP System Manager verwendet wird, um StorageGRID als Cloud-Ebene hinzuzufügen. Dieselbe Konfiguration kann auch mit der ONTAP CLI durchgeführt werden. Anweisungen sind unter ["ONTAP Dokumentation für FabricPool"](#) zu finden.

Schritte

1. Greifen Sie auf System Manager für den ONTAP Cluster zu, zu dem eine Tiering-Verbindung zu StorageGRID hergestellt werden soll.
2. Als Administrator für den Cluster anmelden.
3. Zu **SPEICHER > Ebenen > Cloud-Ebene hinzufügen** navigieren.
4. **StorageGRID** aus der Liste der Objektspeicher-Anbieter auswählen.

StorageGRID-Werte eingeben

Siehe ["ONTAP Dokumentation für FabricPool"](#) für weitere Informationen.

Schritte

1. Füllen Sie das Formular „Cloud-Tier hinzufügen“ aus, indem Sie die `ONTAP_FabricPool_settings_bucketname.txt` Datei oder die manuell ermittelten Werte verwenden.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für diese Cloud-Ebene ein. Der Standardwert kann übernommen werden.
URL-Stil	Wenn Sie "konfigurierte S3 Endpoint-Domännennamen", wählen Sie Virtual Hosted-Style URL aus. Path-Style URL ist die Standardeinstellung für ONTAP, jedoch wird für StorageGRID die Verwendung von virtual hosted-style Anfragen empfohlen. Path-Style URL muss verwendet werden, wenn im Feld Server name (FQDN) eine IP-Adresse anstelle eines Domainnamens angegeben wird.
Servername (FQDN)	Geben Sie den vollqualifizierten Domainnamen (FQDN) ein, den Sie für StorageGRID oder die virtuelle IP-Adresse (VIP) für die StorageGRID HA-Gruppe verwenden. Zum Beispiel <code>s3.storagegrid.company.com</code>. Dabei ist Folgendes zu beachten: • Die hier angegebene IP-Adresse oder der Domänenname muss mit dem Zertifikat übereinstimmen, das Sie für den StorageGRID Load Balancer Endpoint hochgeladen oder generiert haben. • Wenn Sie einen Domännennamen angeben, muss der DNS-Eintrag auf jede IP-Adresse verweisen, die Sie für die Verbindung zu StorageGRID verwenden. Siehe "Den DNS-Server konfigurieren".
SSL	Aktiviert (Standardeinstellung).
Objektspeicherzertifikat	Fügen Sie das Zertifikat-PEM ein, das Sie für den StorageGRID Load Balancer-Endpoint verwenden, einschließlich: -----BEGIN CERTIFICATE----- und -----END CERTIFICATE-----. Hinweis: Wenn das StorageGRID-Zertifikat von einer Zwischenzertifizierungsstelle ausgestellt wurde, muss das Zertifikat der Zwischenzertifizierungsstelle bereitgestellt werden. Wenn das StorageGRID-Zertifikat direkt von der Root-CA ausgestellt wurde, muss das Root-CA-Zertifikat bereitgestellt werden.
Port	Geben Sie den Port ein, der vom StorageGRID Load-Balancer-Endpoint verwendet wird. ONTAP wird diesen Port für die Verbindung zu StorageGRID verwenden. Zum Beispiel 10433.
Zugriffsschlüssel und geheimer Schlüssel	Geben Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den Root-Benutzer des StorageGRID Tenant-Kontos ein. Tipp: Wenn in StorageGRID zukünftig ein neuer Zugriffsschlüssel und ein neuer geheimer Zugriffsschlüssel generiert werden, sollten die neuen Schlüssel in ONTAP eingetragen werden, bevor die alten Werte aus StorageGRID gelöscht werden. Andernfalls könnte ONTAP vorübergehend den Zugriff auf StorageGRID verlieren.

Feld	Beschreibung
Containername	Geben Sie den Namen des StorageGRID Buckets ein, den Sie für die Verwendung mit dieser ONTAP Tier erstellt haben.

2. Die endgültige FabricPool Konfiguration in ONTAP abschließen.
 - a. Ein oder mehrere Aggregate werden an die Cloud-Ebene angehängt.
 - b. Optional kann eine Volume-Tiering-Richtlinie erstellt werden.

Konfigurieren Sie DNS-Servereinträge für StorageGRID mit FabricPool

Nach der Konfiguration von Hochverfügbarkeitsgruppen, Load-Balancer-Endpunkten und S3-Endpunktdomännennamen muss sichergestellt werden, dass das DNS die erforderlichen Einträge für StorageGRID enthält. Ein DNS-Eintrag ist für jeden Namen im Sicherheitszertifikat und für jede IP-Adresse, die verwendet werden könnte, erforderlich.

Siehe "[Überlegungen zum Lastausgleich](#)".

DNS-Einträge für StorageGRID Servernamen

Fügen Sie DNS-Einträge hinzu, um den StorageGRID-Servernamen (vollqualifizierte Domain) jeder StorageGRID-IP-Adresse zuzuordnen, die verwendet wird. Die im DNS einzugebenden IP-Adressen hängen davon ab, ob eine HA-Gruppe von Load-Balancing-Knoten verwendet wird:

- Wenn eine HA-Gruppe konfiguriert wurde, stellt ONTAP eine Verbindung zu den virtuellen IP-Adressen dieser HA-Gruppe her.
- Wenn keine HA-Gruppe verwendet wird, kann ONTAP eine Verbindung zum StorageGRID Load Balancer-Dienst über die IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens herstellen.
- Wenn der Servername zu mehr als einer IP-Adresse aufgelöst wird, stellt ONTAP Client-Verbindungen zu allen IP-Adressen her (bis zu maximal 16 IP-Adressen). Die IP-Adressen werden beim Verbindungsaufbau nach dem Round-Robin-Verfahren ausgewählt.

DNS-Einträge für virtuelle Hosted-Style-Anfragen

Wenn "[S3 Endpoint-Domännennamen](#)" definiert wurde und virtuelle gehostete Anfragen verwendet werden, sind DNS-Einträge für alle erforderlichen S3-Endpunkt-Domännennamen hinzuzufügen, einschließlich aller Wildcard-Namen.

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.

Entfernen von FabricPool Daten aus StorageGRID

Wenn Sie die derzeit in StorageGRID gespeicherten FabricPool-Daten entfernen müssen, ist ONTAP zu verwenden, um alle Daten für das FabricPool-Volume abzurufen und sie in die Performance-Ebene zu verschieben.

Bevor Sie beginnen

- Sie haben die Anweisungen und Hinweise in ["Daten in die Performance-Ebene verschieben"](#) überprüft.
- Sie verwenden ONTAP 9.8 oder höher.
- Sie verwenden ein ["unterstützte Webbrowser"](#).
- Sie gehören einer StorageGRID Benutzergruppe für das FabricPool Mandantenkonto an, das über die ["Alle Buckets oder Root-Zugriffsberechtigung verwalten"](#).

Über diese Aufgabe

Diese Anleitung erklärt, wie Daten von StorageGRID zurück zu FabricPool verschoben werden. Dieses Verfahren wird mit ONTAP und StorageGRID Tenant Manager durchgeführt.

Schritte

1. Von ONTAP aus den `volume modify` Befehl ausführen.

Setzen Sie `tiering-policy` auf `none`, um neues Tiering zu stoppen, und setzen Sie `cloud-retrieval-policy` auf `promote`, um alle zuvor nach StorageGRID ausgelagerten Daten zurückzuholen.

Siehe ["Alle Daten von einem FabricPool Volume auf die Leistungsebene verschieben"](#).

2. Warten Sie, bis der Vorgang abgeschlossen ist.

Sie können den `volume object-store` Befehl mit der `tiering` Option verwenden, um ["den Status der Leistungsstufenbeförderung prüfen"](#).

3. Nach Abschluss der Hochstufung erfolgt die Anmeldung im StorageGRID Tenant Manager für das FabricPool Mandantenkonto.
4. **View buckets** im Dashboard auswählen oder **STORAGE (S3) > Buckets**.
5. Bestätigen Sie, dass der FabricPool Bucket jetzt leer ist.

6. Wenn der Eimer leer ist, ["den Bucket löschen"](#).

Nachdem Sie fertig sind

Wenn der Bucket gelöscht wird, kann das Tiering von FabricPool zu StorageGRID nicht mehr fortgesetzt werden. Da die lokale Tier jedoch weiterhin mit der StorageGRID Cloud-Tier verbunden ist, gibt ONTAP System Manager Fehlermeldungen aus, die darauf hinweisen, dass der Bucket nicht erreichbar ist.

Um diese Fehlermeldungen zu vermeiden, kann eine der folgenden Aktionen durchgeführt werden:

- Mit FabricPool Mirror kann eine andere Cloud-Ebene an das Aggregat angebunden werden.
- Die Daten vom FabricPool Aggregat auf ein Nicht-FabricPool Aggregat verschieben und anschließend das nicht verwendete Aggregat löschen.

Siehe ["ONTAP Dokumentation für FabricPool"](#) für Anweisungen.

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.