Konfigurieren Sie FabricPool

StorageGRID

NetApp
October 03, 2025

Inhalt

Konfigurieren Sie FabricPool

Configure StorageGRID for FabricPool: Übersicht

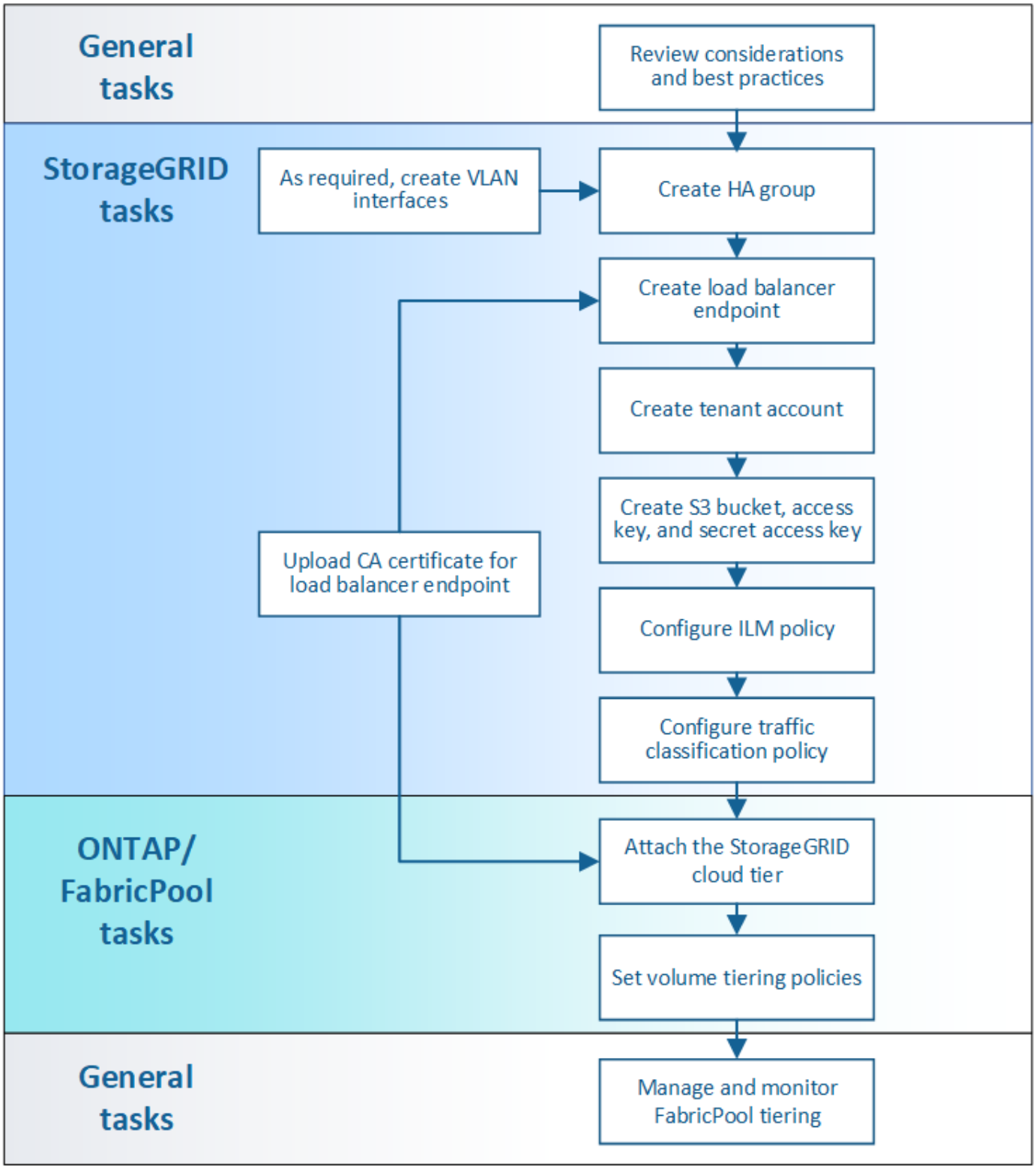
Wenn Sie NetApp ONTAP verwenden, können Sie mit NetApp FabricPool inaktive oder kalte Daten auf einem NetApp StorageGRID Objekt-Storage-System verschieben.

Informationen zu diesen Anweisungen

Mithilfe dieser Anweisungen können Sie:

- Hier erhalten Sie einen Überblick über die Konfiguration eines StorageGRID Objekt-Storage-Systems zur Verwendung mit FabricPool.
- Informieren Sie sich, wie Sie ONTAP Informationen erhalten, wenn Sie StorageGRID als FabricPool Cloud-Tier hinzufügen.
- Best Practices für die Konfiguration der StorageGRID Information Lifecycle Management (ILM)-Richtlinie, einer StorageGRID Traffic-Klassifizierungsrichtlinie und weiterer StorageGRID-Optionen für einen FabricPool-Workload.

Konfigurationsworkflow



Bevor Sie beginnen

- Legen Sie fest, welche FabricPool Volume Tiering-Richtlinie Sie für das Tiering inaktiver ONTAP-Daten an StorageGRID verwenden möchten.
- Planen und installieren Sie ein StorageGRID System, um Ihre Storage-Kapazitäts- und Performance-Anforderungen zu erfüllen.
- Machen Sie sich mit der StorageGRID Systemsoftware vertraut, einschließlich Grid Manager und Tenant

Manager.

- Lesen Sie die folgenden zusätzlichen Ressourcen durch, die Details zur Verwendung und Konfiguration von FabricPool enthalten:
  - "TR-4598: FabricPool Best Practices in ONTAP 9.9.1"
  - "ONTAP 9-Dokumentation"

Was ist FabricPool?

FabricPool ist eine ONTAP Hybrid-Storage-Lösung mit einem hochperformanten Flash-Aggregat als Performance-Tier und einem Objektspeicher als Cloud-Tier. Daten werden entweder auf dem primären Storage-Medium oder im Objekt-Datastore gespeichert, je nachdem, ob der Zugriff häufig erfolgt oder nicht. Mit FabricPool-fähigen Aggregaten senken Sie die Storage-Kosten, ohne dabei Einbußen bei Performance, Effizienz oder Sicherung hinnehmen zu müssen.

Es sind keine Änderungen an der Architektur erforderlich und die Daten- und Applikationsumgebung lässt sich weiterhin über das zentrale ONTAP Storage-System managen.

Was ist StorageGRID?

StorageGRID ist eine Storage-Architektur, die Daten als Objekte managt und nicht als andere Storage-Architekturen wie Datei- oder Block-Storage. Objekte werden in einem einzelnen Container (z. B. in einem Bucket) aufbewahrt und sind nicht als Dateien in einem Verzeichnis in anderen Verzeichnissen verschachtelt. Obwohl Objekt-Storage im Allgemeinen eine geringere Performance als Datei- oder Block-Storage bietet, ist sie deutlich skalierbarer. StorageGRID Buckets können Daten im Petabyte-Bereich und Milliarden Objekte enthalten.

Vorteile von StorageGRID als Cloud-Tier von FabricPool

FabricPool kann ONTAP Daten zu verschiedenen Objektspeicher-Providern, einschließlich StorageGRID, verschieben. Im Gegensatz zu Public Clouds, bei denen eine maximale Anzahl unterstützter IOPS (Input/Output Operations per Second) auf Bucket- oder Container-Ebene festgelegt werden kann, lässt sich die StorageGRID-Performance mit der Anzahl der Nodes in einem System skalieren. Durch den Einsatz von StorageGRID als FabricPool Cloud-Tier können kalte Daten in Ihrer eigenen Private Cloud vorgehalten werden, um höchste Performance und vollständige Kontrolle über Ihre Daten zu erzielen.

Zudem ist keine FabricPool Lizenz erforderlich, wenn Sie StorageGRID als Cloud-Tier verwenden.

Kann ich mit StorageGRID mehrere ONTAP Cluster verwenden?

In diesen Anweisungen wird beschrieben, wie StorageGRID mit einem einzelnen ONTAP Cluster verbunden werden. Es empfiehlt sich jedoch, dasselbe StorageGRID System mit mehreren ONTAP Clustern zu verbinden.

Die einzige Voraussetzung für das Tiering von Daten zwischen mehreren ONTAP Clustern zu einem einzelnen StorageGRID System ist, dass Sie für jedes Cluster einen anderen S3 Bucket verwenden müssen. Je nach Ihren Anforderungen können Sie für alle Cluster dieselbe HA-Gruppe (High Availability, HA-Gruppe), einen Load Balancer-Endpunkt und ein Mandantenkonto verwenden. Alternativ können Sie jede dieser Elemente für jedes Cluster konfigurieren.

StorageGRID als Cloud-Tier hinzufügen

Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier

Bevor Sie StorageGRID als Cloud Tier für FabricPool hinzufügen können, müssen Sie einige Konfigurationsschritte in StorageGRID ausführen, um bestimmte Werte zu erhalten.

Über diese Aufgabe

In der folgenden Tabelle werden die Informationen aufgeführt, die Sie ONTAP bereitstellen müssen, wenn Sie StorageGRID als Cloud-Tier für FabricPool anhängen. In den Themen in diesem Abschnitt wird erläutert, wie Sie den StorageGRID Grid Manager und den Tenant Manager verwenden, um die Informationen zu erhalten, die Sie benötigen.

> Die genauen Feldnamen und der Prozess, den Sie zur Eingabe der erforderlichen Werte in ONTAP verwenden, hängen davon ab, ob Sie die ONTAP CLI (Storage Aggregate object-Store config create) oder ONTAP System Manager (**Storage Aggregate Disks Cloud Tier**) verwenden.

Weitere Informationen finden Sie im Folgenden:

- "TR-4598: FabricPool Best Practices in ONTAP 9.9.1"
- "ONTAP 9-Dokumentation"

ONTAP Field	Beschreibung
Objektspeichername	Jeder eindeutige und beschreibende Name. Beispiel: `StorageGRID_Cloud_Tier`.
Anbietertyp	StorageGRID (ONTAP System Manager) oder `SGWS` (ONTAP CLI).
Port	Der Port, den FabricPool verwenden wird, wenn er eine Verbindung zu StorageGRID herstellt. Sie legen fest, welche Portnummer beim Definieren des StorageGRID Load Balancer-Endpunkts verwendet werden soll. Erstellen eines Load Balancer-Endpunkts für FabricPool

ONTAP Field	Beschreibung
Servername	Der vollständig qualifizierte Domänenname (FQDN) für den StorageGRID Load Balancer-Endpunkt. Beispiel: `s3.storagegrid.company.com`. Beachten Sie Folgendes: • Der hier angegebene Domänenname muss mit dem Domänennamen auf dem CA-Zertifikat übereinstimmen, das Sie für den StorageGRID Load Balancer-Endpunkt hochladen. • Der DNS-Datensatz für diesen Domain-Namen muss jeder IP-Adresse zugeordnet werden, die Sie zum Herstellen einer Verbindung zu StorageGRID verwenden werden. Konfigurieren Sie den DNS-Server für StorageGRID-IP-Adressen
Containername	Der Name des StorageGRID-Buckets, den Sie mit diesem ONTAP-Cluster verwenden werden. Beispiel: `fabricpool-bucket`. Sie können diesen Bucket im Mandanten-Manager erstellen oder, beginnend mit ONTAP 9.10 System Manager, Sie können den Bucket mit dem FabricPool-Setup-Assistenten erstellen. Beachten Sie Folgendes: • Der Bucket-Name kann nach dem Erstellen der Konfiguration nicht mehr geändert werden. • Für den Bucket ist die Versionierung nicht aktiviert. • Sie müssen einen anderen Bucket für jedes ONTAP Cluster verwenden, für das Daten in StorageGRID verschoben werden sollen. Erstellen eines S3-Buckets und Abrufen eines Zugriffsschlüssels
Zugriffsschlüssel und geheimes Passwort	Der Zugriffsschlüssel und der geheime Zugriffsschlüssel für das StorageGRID-Mandantenkonto. Diese Werte generieren Sie im Tenant Manager. Erstellen eines S3-Buckets und Abrufen eines Zugriffsschlüssels
SSL	Muss aktiviert sein.

ONTAP Field	Beschreibung
Objektspeicherzertifikat	Das CA-Zertifikat, das Sie beim Erstellen des StorageGRID Load Balancer-Endpunkts hochgeladen haben. **Hinweis:** Wenn eine Zwischenzertifizierungsstelle das StorageGRID-Zertifikat ausgestellt hat, müssen Sie das Zwischenzertifikat vorlegen. Wenn das StorageGRID-Zertifikat direkt von der Root-CA ausgestellt wurde, müssen Sie das Root-CA-Zertifikat bereitstellen. Erstellen eines Load Balancer-Endpunkts für FabricPool

Nachdem Sie fertig sind

Nachdem Sie die erforderlichen StorageGRID Informationen erhalten haben, können Sie unter ONTAP StorageGRID als Cloud-Tier hinzufügen, die Cloud-Ebene als Aggregat hinzufügen und die Tiering-Richtlinien für Volumes festlegen.

Best Practices für den Lastausgleich

Bevor Sie StorageGRID als FabricPool-Cloud-Tier anhängen können, müssen Sie mit StorageGRID Grid Manager mindestens einen Load Balancer-Endpunkt konfigurieren.

Was ist Load Balancing?

Wenn Daten vom FabricPool zu einem StorageGRID System verschoben werden, verwendet StorageGRID einen Load Balancer zum Managen des Aufnahme- und Abrufs-Workloads. Der Lastausgleich maximiert die Geschwindigkeit und die Verbindungskapazität, indem der FabricPool Workload auf mehrere Storage-Nodes verteilt wird.

Der StorageGRID Load Balancer-Service wird auf allen Admin-Nodes und allen Gateway-Knoten installiert und bietet Layer 7-Lastausgleich. Sie beendet die TLS-Beendigung von Client-Anforderungen, prüft die Anforderungen und stellt neue sichere Verbindungen zu den Storage-Nodes her.

Der Load Balancer-Service auf jedem Node wird unabhängig ausgeführt, wenn der Client-Datenverkehr an die Storage Nodes weitergeleitet wird. Durch eine Gewichtung leitet der Load Balancer-Service mehr Anfragen an Storage-Nodes mit höherer CPU-Verfügbarkeit weiter.

Obwohl der StorageGRID Load Balancer-Service der empfohlene Load-Balancing-Mechanismus ist, können Sie stattdessen einen Load Balancer eines Drittanbieters integrieren. Weitere Informationen erhalten Sie von Ihrem NetApp Ansprechpartner oder unter "TR-4626: StorageGRID Anbieter- und Global Load Balancer".

> Der separate Connection Load Balancer (CLB)-Service auf Gateway-Nodes ist veraltet und wird nicht mehr für die Verwendung mit FabricPool empfohlen.

Best Practices für den StorageGRID-Lastausgleich

Als allgemeine Best Practice sollte jeder Standort in Ihrem StorageGRID-System zwei oder mehr Nodes mit dem Load Balancer Service umfassen. Ein Standort kann beispielsweise zwei Gateway-Nodes oder einen Admin-Node und einen Gateway-Node umfassen. Vergewissern Sie sich, dass für jeden Load-Balancing-Node eine entsprechende Netzwerk-, Hardware- oder Virtualisierungsinfrastruktur vorhanden ist, unabhängig davon, ob Sie SG100- oder SG1000-Servicegeräte, Bare Metal-Nodes oder VM-basierte Nodes verwenden.

Sie müssen einen StorageGRID Load Balancer-Endpunkt konfigurieren, um den Port zu definieren, den Gateway-Knoten und Admin-Knoten für eingehende und ausgehende FabricPool-Anforderungen verwenden werden.

Best Practices für das Endpoint-Zertifikat für Load Balancer

Wenn Sie einen Endpunkt für den Load Balancer für die Verwendung mit FabricPool erstellen, sollten Sie HTTPS als Protokoll verwenden. Eine Kommunikation mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, wird jedoch nicht empfohlen

Anschließend können Sie entweder ein Zertifikat hochladen, das entweder von einer öffentlichen vertrauenswürdigen oder einer privaten Zertifizierungsstelle signiert ist, oder ein selbstsigniertes Zertifikat generieren. Mit dem Zertifikat kann ONTAP sich mit StorageGRID authentifizieren.

Als Best Practice sollten Sie ein CA-Serverzertifikat verwenden, um die Verbindung zu sichern. Von einer Zertifizierungsstelle signierte Zertifikate können unterbrechungsfrei gedreht werden.

Wenn Sie ein CA-Zertifikat zur Verwendung mit dem Endpunkt des Load Balancer anfordern, stellen Sie sicher, dass der Domänenname auf dem Zertifikat mit dem in ONTAP eingegebenen Servernamen für diesen Load Balancer-Endpunkt übereinstimmt. Wenn möglich, verwenden Sie einen Platzhalter (*), um virtuelle URLs im Hoststil zu ermöglichen. Beispiel:

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

Wenn Sie StorageGRID als FabricPool Cloud Tier hinzufügen, müssen Sie beim ONTAP Cluster dasselbe Zertifikat sowie die Zertifikate „Root“ und „untergeordnete Certificate Authority“ (CA) installieren.

> ⓘ StorageGRID verwendet Serverzertifikate aus verschiedenen Gründen. Wenn Sie eine Verbindung zum Load Balancer Service herstellen, können Sie optional das S3- und Swift-API-Zertifikat verwenden.

Weitere Informationen zum Serverzertifikat für einen Lastausgleichsendpunkt:

- Konfigurieren von Load Balancer-Endpunkten
- Härtungsrichtlinien für Serverzertifikate

Best Practices für Hochverfügbarkeitsgruppen

Bevor Sie StorageGRID als FabricPool Cloud-Tier anhängen, sollten Sie StorageGRID Grid Manager zur Konfiguration einer HA-Gruppe (High Availability, Hochverfügbarkeit) verwenden.

Was ist eine HA-Gruppe (High Availability, Hochverfügbarkeit)?

Um sicherzustellen, dass der Load Balancer-Service zum Verwalten von FabricPool-Daten immer verfügbar ist, können Sie die Netzwerkschnittstellen mehrerer Admin- und Gateway-Nodes zu einer einzigen Einheit gruppieren, die als HA-Gruppe (High Availability, Hochverfügbarkeit) bezeichnet wird. Wenn der aktive Node in der HA-Gruppe ausfällt, kann der Workload weiterhin von einem anderen Node in der Gruppe gemanagt werden.

Jede HA-Gruppe ermöglicht einen hochverfügbaren Zugriff auf die Shared Services auf den zugehörigen

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

Zum Erstellen einer HA-Gruppe führen Sie die folgenden allgemeinen Schritte aus:

1. Wählen Sie Netzwerkschnittstellen für einen oder mehrere Admin-Nodes oder Gateway-Nodes aus. Sie können die Grid Network Interface (eth0), die Client Network Interface (eth2) oder eine VLAN-Schnittstelle auswählen.

   > Wenn Sie eine VLAN-Schnittstelle zur Trennung des FabricPool-Datenverkehrs verwenden möchten, muss ein Netzwerkadministrator zunächst eine Trunk-Schnittstelle und das entsprechende VLAN konfigurieren. Jedes VLAN wird durch eine numerische ID oder ein Tag identifiziert. Beispielsweise könnte Ihr Netzwerk VLAN 100 für FabricPool-Datenverkehr verwenden.

2. Weisen Sie der Gruppe eine oder mehrere virtuelle IP-Adressen (VIP) zu. Clients, z. B. FabricPool, können eine dieser VIP-Adressen verwenden, um eine Verbindung zu StorageGRID herzustellen.
3. Geben Sie eine Schnittstelle für die primäre Schnittstelle an, und bestimmen Sie die Prioritätsreihenfolge für alle Backup-Schnittstellen. Die primäre Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.

Wenn die HA-Gruppe mehrere Schnittstellen umfasst und die primäre Schnittstelle ausfällt, werden die VIP-Adressen auf die erste Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. Wenn diese Schnittstelle ausfällt, wechseln die VIP-Adressen zur nächsten Backup-Schnittstelle usw. Dieser Failover-Prozess dauert in der Regel nur wenige Sekunden und ist schnell genug, dass Client-Applikationen nur geringe Auswirkungen haben und sich auf normale Wiederholungsmuster verlassen können, um den Betrieb fortzusetzen.

Wenn der Fehler behoben ist und eine Schnittstelle mit höherer Priorität wieder verfügbar wird, werden die VIP-Adressen automatisch auf die Schnittstelle mit der höchsten Priorität verschoben, die verfügbar ist.

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

Die Best Practices zum Erstellen einer StorageGRID HA-Gruppe für FabricPool hängen vom Workload ab:

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

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

Konfigurieren Sie den DNS-Server für StorageGRID-IP-Adressen

Nach der Konfiguration von Hochverfügbarkeitsgruppen und Endpunkten des Load Balancer müssen Sie sicherstellen, dass das DNS (Domain Name System) für das ONTAP-System einen Datensatz enthält, um den StorageGRID-Servernamen (vollständig

qualifizierter Domänenname) der IP-Adresse zuzuordnen, die FabricPool zum Herstellen von Verbindungen verwendet.

Die IP-Adresse, die Sie im DNS-Datensatz eingeben, hängt davon ab, ob Sie eine HA-Gruppe von Load-Balancing-Nodes verwenden:

- Wenn Sie eine HA-Gruppe konfiguriert haben, stellt FabricPool eine Verbindung zu den virtuellen IP-Adressen dieser HA-Gruppe her.
- Wenn Sie keine HA-Gruppe verwenden, kann sich FabricPool mithilfe der IP-Adresse eines beliebigen Gateway-Node oder Admin-Node mit dem StorageGRID Load Balancer-Service verbinden.

Außerdem müssen Sie sicherstellen, dass der DNS-Datensatz alle erforderlichen Endpunkt-Domain-Namen referenziert, einschließlich Platzhalternamen.

Erstellen einer HA-Gruppe (High Availability, Hochverfügbarkeit) für FabricPool

Wenn Sie StorageGRID für die Verwendung mit FabricPool konfigurieren, können Sie optional eine oder mehrere HA-Gruppen (High Availability, Hochverfügbarkeit) erstellen. Eine HA-Gruppe besteht aus mindestens einer Netzwerkschnittstellen auf Admin-Nodes, Gateway-Nodes oder beiden.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Berechtigung Root Access.
- Wenn Sie ein VLAN verwenden möchten, haben Sie die VLAN-Schnittstelle erstellt. Siehe Konfigurieren Sie die VLAN-Schnittstellen.

Über diese Aufgabe

Jede HA-Gruppe verwendet virtuelle IP-Adressen (VIPs), um hochverfügbaren Zugriff auf die Shared Services auf den zugehörigen Nodes zu ermöglichen.

Weitere Informationen zu dieser Aufgabe finden Sie unter Management von Hochverfügbarkeitsgruppen.

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk Hochverfügbarkeitsgruppen**.
2. Wählen Sie **Erstellen**.
3. Geben Sie einen eindeutigen Namen und optional eine Beschreibung ein.
4. Wählen Sie eine oder mehrere Schnittstellen aus, die dieser HA-Gruppe hinzugefügt werden sollen.

   Verwenden Sie die Spaltenüberschriften, um die Zeilen zu sortieren, oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.

5. Ermitteln Sie die primäre Schnittstelle und alle Backup-Schnittstellen für diese HA-Gruppe.

   Ziehen Sie Zeilen per Drag-and-Drop, um die Werte in der Spalte **Priority Order** zu ändern.

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

   Wenn die HA-Gruppe mehr als eine Schnittstelle enthält und die aktive Schnittstelle ausfällt, verschieben

die VIP-Adressen auf die erste Backup-Schnittstelle in der Prioritätsreihenfolge. Wenn diese Schnittstelle ausfällt, wechseln die VIP-Adressen zur nächsten Backup-Schnittstelle usw. Wenn Ausfälle behoben werden, werden die VIP-Adressen wieder auf die Schnittstelle mit der höchsten Priorität verschoben, die verfügbar ist.

6. Geben Sie das VIP-Subnetz in CIDR-Notation#8212;eine IPv4-Adresse, gefolgt von einem Schrägstrich und der Subnetz-Länge (0-32) an.

   Die Netzwerkadresse darf keine Host-Bits festgelegt haben. Beispiel: `192.16.0.0/22`.

7. Wenn sich die für den Zugriff auf StorageGRID verwendeten ONTAP-IP-Adressen nicht im gleichen Subnetz wie die StorageGRID-VIP-Adressen befinden, geben Sie optional die lokale Gateway-IP-Adresse für StorageGRID VIP ein. Die IP-Adresse des lokalen Gateways muss sich im VIP-Subnetz befinden.
8. Geben Sie eine oder mehrere virtuelle IP-Adressen für die HA-Gruppe ein. Sie können bis zu 10 IP-Adressen hinzufügen. Alle VIPs müssen sich im VIP-Subnetz befinden.

   Sie müssen mindestens eine IPv4-Adresse angeben. Optional können Sie weitere IPv4- und IPv6-Adressen angeben.

9. Wählen Sie **HA-Gruppe erstellen** und dann **Fertig stellen**.

Erstellen eines Load Balancer-Endpunkts für FabricPool

Wenn Sie StorageGRID für die Verwendung mit FabricPool konfigurieren, müssen Sie einen Endpunkt für den Load Balancer konfigurieren und das Endpoint-Zertifikat für den Load Balancer hochladen, das zum Sichern der Verbindung zwischen ONTAP und StorageGRID verwendet wird.

Was Sie benötigen

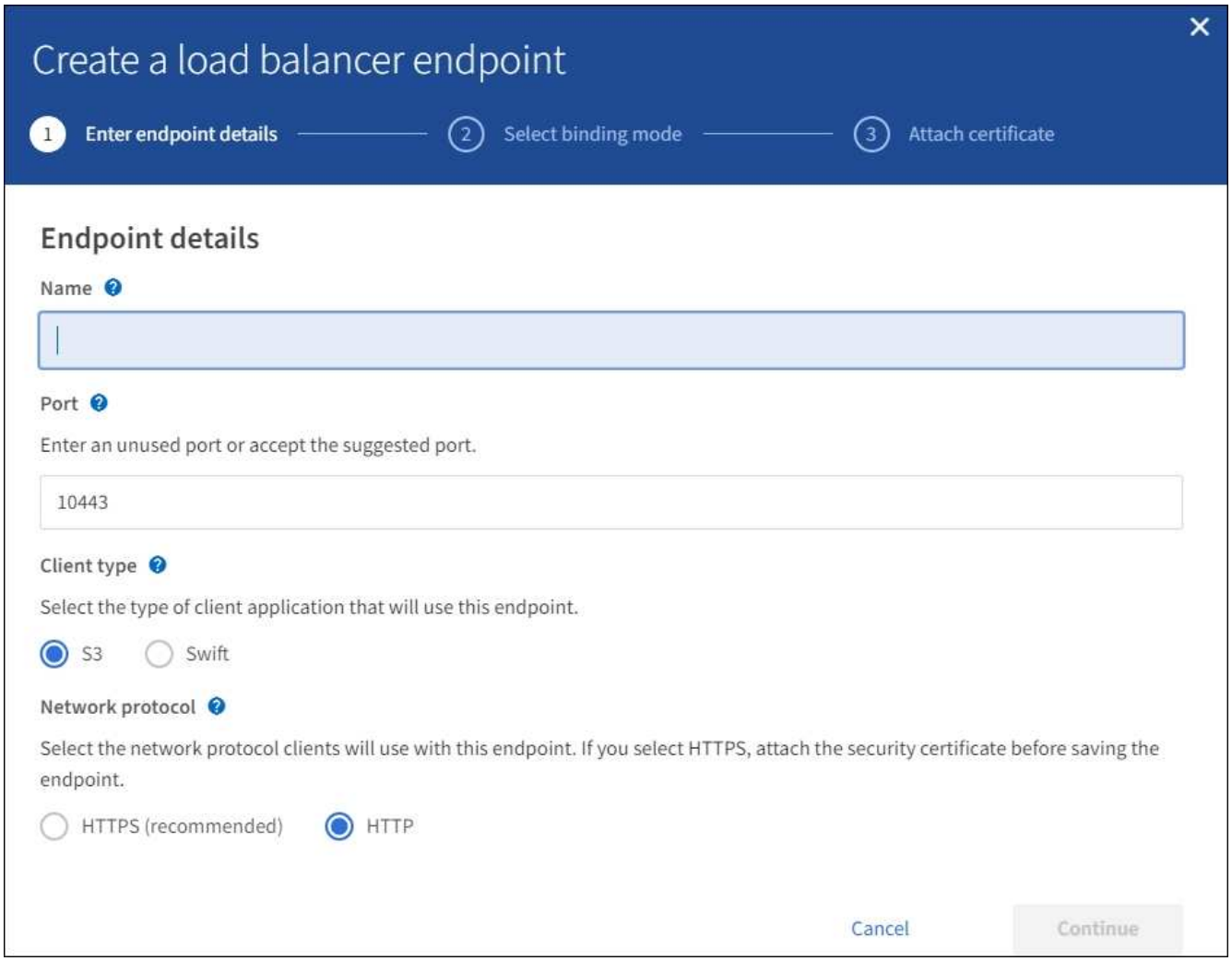
- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Root-Zugriffsberechtigung.
- Sie haben die folgenden Dateien:
  - Serverzertifikat: Die benutzerdefinierte Serverzertifikatdatei.
  - Server Certificate Private Key: Die private Schlüsseldatei des benutzerdefinierten Serverzertifikats.
  - CA-Paket: Eine einzelne optionale Datei, die die Zertifikate jeder Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.

Über diese Aufgabe

Weitere Informationen zu dieser Aufgabe finden Sie unter Konfigurieren von Load Balancer-Endpunkten.

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk Load Balancer-Endpunkte** aus.
2. Wählen Sie **Erstellen**.



3. Geben Sie Details zu Endpunkten ein.

Feld	Beschreibung
Name	Einen beschreibenden Namen für den Endpunkt
Port	Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist standardmäßig auf 10433 eingestellt, Sie können jedoch alle nicht verwendeten externen Ports eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Knoten konfiguriert, da diese Ports auf Admin-Nodes reserviert sind. **Hinweis:** Ports, die von anderen Netzdiensten verwendet werden, sind nicht zulässig. SieheReferenz für Netzwerk-Ports. Sie müssen diese Portnummer an ONTAP angeben, wenn Sie StorageGRID als FabricPool Cloud Tier anhängen.
Client-Typ	Wählen Sie **S3**.

Feld	Beschreibung
Netzwerkprotokoll	Wählen Sie **HTTPS**. **Hinweis**: Die Verwendung von **HTTP** wird unterstützt, aber nicht empfohlen.

4. Wählen Sie **Weiter**.
5. Geben Sie den Bindungsmodus an.

   Verwenden Sie die **Global**-Einstellung (empfohlen) oder beschränken Sie die Zugänglichkeit dieses Endpunkts auf einen der folgenden Elemente:

   - Spezielle Netzwerkschnittstellen bestimmter Nodes.
   - Spezifische virtuelle Hochverfügbarkeits-IP-Adressen (VIPs). Verwenden Sie diese Auswahl nur, wenn ein deutlich höheres Maß an Isolierung von Workloads erforderlich ist.
6. Wählen Sie **Weiter**.
7. Wählen Sie **Zertifikat hochladen** (empfohlen) und navigieren Sie anschließend zu Ihrem Serverzertifikat, Ihrem privaten Zertifikatschlüssel und dem optionalen CA-Paket.
8. Wählen Sie **Erstellen**.

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

Erstellen eines Mandantenkontos für FabricPool

Sie müssen ein Mandantenkonto im Grid Manager for FabricPool Use erstellen.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Mandantenkonten ermöglichen Client-Applikationen, Objekte auf StorageGRID zu speichern und abzurufen. Jedes Mandantenkonto verfügt über eine eigene Account-ID, autorisierte Gruppen und Benutzer, Buckets und Objekte.

Sie können dasselbe Mandantenkonto für mehrere ONTAP Cluster verwenden. Oder Sie können bei Bedarf ein dediziertes Mandantenkonto für jedes ONTAP Cluster erstellen.

Bei diesen Anweisungen wird davon ausgegangen, dass Sie Single Sign-On (SSO) für den Grid Manager konfiguriert haben. Wenn SSO nicht aktiviert ist, verwenden Sie Diese Anweisungen zum Erstellen eines Mandantenkontos Stattdessen.

Schritte

1. Wählen Sie **MIETER**.
2. Wählen Sie **Erstellen**.
3. Geben Sie einen Anzeigenamen und eine Beschreibung ein.

4. Wählen Sie **S3**.
5. Lassen Sie das Feld **Storage Quota** leer.
6. Wählen Sie **Plattformdienste zulassen** aus, um die Nutzung von Plattformdiensten zu ermöglichen.

   Wenn Plattformservices aktiviert sind, kann ein Mandant Funktionen wie CloudMirror Replizierung verwenden, die auf externe Services zugreifen.

7. Wählen Sie nicht **eigene Identitätsquelle verwenden** aus.
8. Wählen Sie nicht **S3 Select zulassen** aus.
9. Wählen Sie eine vorhandene föderierte Gruppe aus dem Grid Manager aus, um die ursprüngliche Root-Zugriffsberechtigung für den Mandanten zu erhalten.
10. Wählen Sie **Create Tenant**.

Erstellen eines S3-Buckets und Abrufen eines Zugriffsschlüssels

Bevor Sie StorageGRID mit einem FabricPool-Workload verwenden, müssen Sie einen S3-Bucket für Ihre FabricPool-Daten erstellen. Außerdem müssen Sie einen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel für das Mandantenkonto erhalten, das Sie für FabricPool verwenden werden.

Was Sie benötigen

- Sie haben ein Mandantenkonto für die Nutzung von FabricPool erstellt.

Über diese Aufgabe

In diesen Anweisungen wird die Verwendung von StorageGRID Mandanten-Manager zur Erstellung eines Buckets beschrieben und Zugriffschlüssel erhalten. Sie können diese Aufgaben auch mit der Mandantenmanagement-API oder der StorageGRID S3 REST-API ausführen. Oder, wenn Sie ONTAP 9.10 verwenden, können Sie den Bucket stattdessen mit dem FabricPool-Setup-Assistenten erstellen.

Weitere Informationen:

- Verwenden Sie ein Mandantenkonto
- S3 verwenden

Schritte

1. Melden Sie sich beim Tenant Manager an.

   Sie können eine der folgenden Aktionen ausführen:

   - Wählen Sie auf der Seite Mandantenkonten im Grid Manager den Link **Anmelden** für den Mieter aus, und geben Sie Ihre Anmeldedaten ein.
   - Geben Sie die URL für das Mandantenkonto in einem Webbrowser ein, und geben Sie Ihre Anmeldedaten ein.

2. Erstellung eines S3-Buckets für FabricPool-Daten

   Sie müssen für jedes zu verwendende ONTAP Cluster einen eindeutigen Bucket erstellen.

   a. Wählen Sie **STORAGE (S3) Buckets** aus.
   b. Wählen Sie **Eimer erstellen**.

c. Geben Sie den Namen des StorageGRID-Buckets ein, den Sie mit FabricPool verwenden möchten. Beispiel: `fabricpool-bucket`.

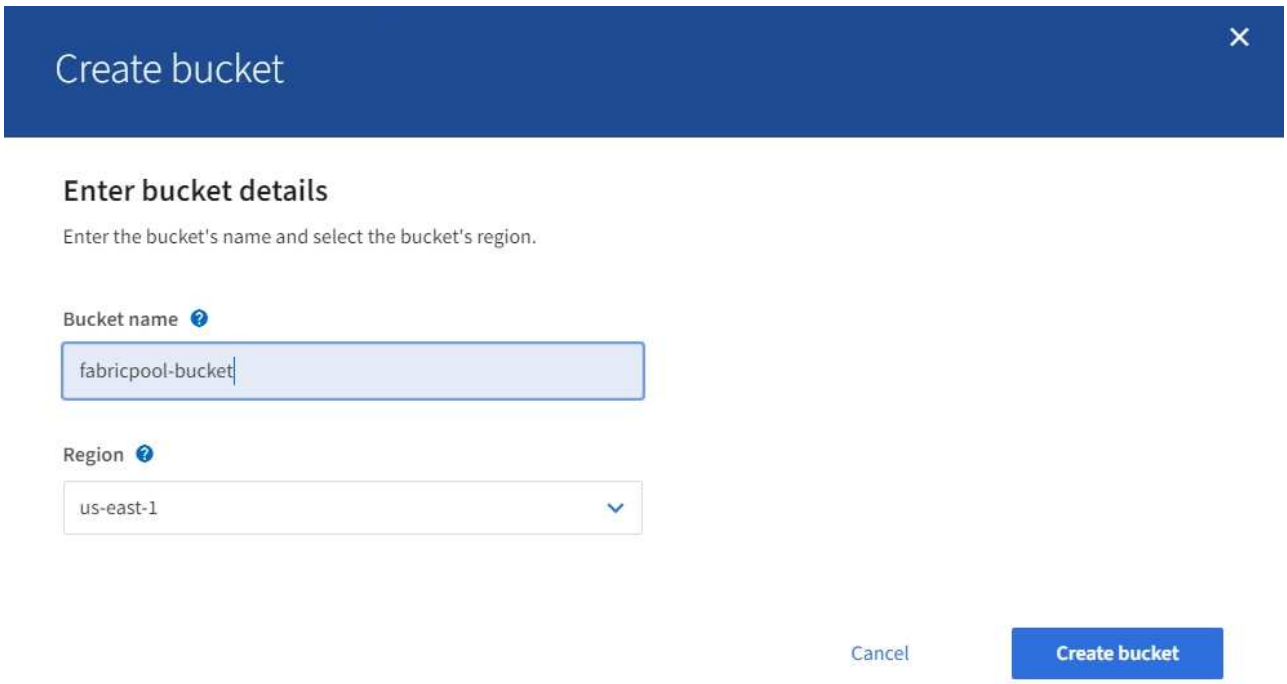
> Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht ändern.

Bucket-Namen müssen folgende Regeln einhalten:

- Jedes StorageGRID System muss eindeutig sein (nicht nur innerhalb des Mandantenkontos).
- Muss DNS-konform sein.
- Darf mindestens 3 und nicht mehr als 63 Zeichen enthalten.
- Kann eine Reihe von einer oder mehreren Etiketten sein, wobei angrenzende Etiketten durch einen Zeitraum getrennt sind. Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden. Es können nur Kleinbuchstaben, Ziffern und Bindestriche verwendet werden.
- Darf nicht wie eine Text-formatierte IP-Adresse aussehen.
- Perioden sollten nicht in Anforderungen im virtuellen gehosteten Stil verwendet werden. Perioden verursachen Probleme bei der Überprüfung des Server-Platzhalterzertifikats.

d. Wählen Sie die Region für diesen Bucket aus.

Standardmäßig werden alle Buckets im erstellt `us-east-1` Werden.



e. Wählen Sie **Eimer erstellen**.

> Für FabricPool Buckets ist die empfohlene Bucket-Konsistenzstufe **Read-after-New-write**, was die Standardeinstellung für einen neuen Bucket ist. Bearbeiten Sie FabricPool Buckets nicht, um **available** oder eine andere Konsistenzstufe zu verwenden.

3. Erstellen Sie einen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel.

a. Wählen Sie **STORAGE (S3) Meine Zugriffsschlüssel** aus.

b. Wählen Sie **Schlüssel erstellen**.

c. Wählen Sie **Zugriffsschlüssel erstellen**.

d. Kopieren Sie die Zugriffsschlüssel-ID und den Schlüssel für den geheimen Zugriff an einen sicheren Ort, oder wählen Sie **.csv herunterladen**, um eine Tabellenkalkulationsdatei mit der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel zu speichern.

   Sie geben diese Werte in ONTAP ein, wenn Sie StorageGRID als FabricPool Cloud-Tier konfigurieren.

> ⓘ Wenn Sie in Zukunft einen neuen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel erstellen, vergessen Sie nicht, die entsprechenden Werte in ONTAP sofort zu aktualisieren, um sicherzustellen, dass ONTAP Daten unterbrechungsfrei in StorageGRID speichern und abrufen kann.

Nutzen Sie das Information Lifecycle Management von StorageGRID mit FabricPool-Daten

Wenn Sie FabricPool für das Tiering von Daten zu StorageGRID verwenden, müssen Sie die Anforderungen für die Erstellung von StorageGRID Information Lifecycle Management (ILM)-Regeln und eine ILM-Richtlinie für das Management von FabricPool-Daten kennen. Sie müssen sicherstellen, dass die ILM-Regeln für FabricPool Daten nicht von Unterbrechungen geprägt sind.

> ⓘ FabricPool ist nicht mit den StorageGRID ILM-Regeln oder -Richtlinien bekannt. Wenn die StorageGRID ILM-Richtlinie falsch konfiguriert ist, kann es zu Datenverlusten kommen. Siehe Objektmanagement mit ILM Für detaillierte ILM-Anweisungen.

Diese Richtlinien prüfen, um sicherzustellen, dass Ihre ILM-Regeln und ILM-Richtlinien für FabricPool Daten und Ihre geschäftlichen Anforderungen geeignet sind. Wenn Sie bereits StorageGRID ILM verwenden, müssen Sie möglicherweise Ihre aktive ILM-Richtlinie aktualisieren, um diese Richtlinien zu erfüllen.

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

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

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

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

- Verwenden Sie keine ILM-Regel, die Daten des FabricPool Cloud-Tiers ablaufen oder löschen soll. Legen Sie die Aufbewahrungsdauer in jeder ILM-Regel auf „Forever“ fest, um zu gewährleisten, dass FabricPool-Objekte nicht durch StorageGRID ILM gelöscht werden.
- Erstellen Sie keine Regeln, nach denen FabricPool Cloud-Tiering-Daten aus dem Bucket in einen anderen Speicherort verschoben werden. Mit ILM-Regeln können FabricPool-Daten nicht mithilfe eines Archivierungs-Nodes auf Band archiviert werden. Alternativ können Sie zum Verschieben von FabricPool-Daten in einen anderen Objektspeicher einen Cloud-Storage-Pool verwenden.

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

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

Beispiel für eine ILM-Richtlinie für FabricPool-Daten

Nutzen Sie diese einfache Beispielrichtlinie als Ausgangspunkt für Ihre eigenen ILM-Regeln und -Richtlinien.

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

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen. Weitere Informationen finden Sie unter Objektmanagement mit ILM.

Schritte

1. Erstellen Sie einen Speicherpool mit dem Namen **DEN**. Wählen Sie den Standort Denver aus.
2. Erstellen Sie ein Erasure-Coding-Profil mit dem Namen **2 plus 1**. Wählen Sie die 2+1-Löschcodierung und den **DEN**-Speicherpool aus.
3. Erstellen einer ILM-Regel, die sich nur auf die Daten in bezieht `fabricpool-bucket`. In dieser Beispielregel werden Kopien mit Verfahren zur Fehlerkorrektur erstellt.

Regeldefinition	Beispielwert
Regelname	2 plus 1 Erasure Coding für FabricPool-Daten
Bucket-Name	`fabricpool-bucket` Sie könnten auch nach dem FabricPool-Mandantenkonto filtern.

Regeldefinition	Beispielwert
Erweiterte Filterung	Objektgröße (MB) größer als 0.2 MB. **Hinweis:** FabricPool schreibt nur 4 MB Objekte, aber Sie müssen einen Filter für Objektgröße hinzufügen, da diese Regel das Erasure Coding verwendet.
Referenzzeit	Aufnahmezeit
Platzierung	Ab Tag 0 dauerhaft speichern
Typ	Erasure Coding
Standort	DEN (2 plus 1)
Aufnahmeverhalten	Ausgeglichen

4. Erstellen einer ILM-Regel, die zwei replizierte Kopien von Objekten erstellt, die nicht mit der ersten Regel übereinstimmt. Wählen Sie keinen grundlegenden Filter (Mandantenkonto oder Bucket-Name) oder erweiterte Filter aus.

Regeldefinition	Beispielwert
Regelname	Zwei replizierte Kopien
Bucket-Name	*None*
Erweiterte Filterung	*None*
Referenzzeit	Aufnahmezeit
Platzierung	Ab Tag 0 dauerhaft speichern
Typ	Datenreplizierung
Standort	DEN
Kopien	2
Aufnahmeverhalten	Ausgeglichen

5. Erstellen Sie eine vorgeschlagene ILM-Richtlinie und wählen Sie beide Regeln aus. Da die Replikationsregel keine Filter verwendet, kann es sich um die Standardregel (letzte) für die Richtlinie handelt.
6. Aufnahme von Testobjekten in das Raster

7. Simulieren Sie die Richtlinie mit den Testobjekten, um das Verhalten zu überprüfen.
8. Aktivieren Sie die Richtlinie.

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

- Die Daten-Tiering von FabricPool in `fabricpool-bucket` Wird mithilfe des 2+1-Schemas zur Einhaltung von Datenkonsistenz (Erasure Coding) codiert. Zwei Datenfragmente und ein Paritätsfragment werden auf drei verschiedenen Storage Nodes platziert.
- Alle Objekte in allen anderen Buckets werden repliziert. Es werden zwei Kopien erstellt und auf zwei verschiedenen Speicherknoten platziert.
- Die von Erasure Coding und replizierten Kopien werden in StorageGRID aufbewahrt, bis sie vom S3 Client gelöscht werden. StorageGRID ILM löscht diese Elemente nie.

Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool

Optional können Sie eine StorageGRID Traffic-Klassifizierungsrichtlinie entwerfen, um die Servicequalität für den FabricPool-Workload zu optimieren.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Berechtigung Root Access.

Über diese Aufgabe

Die Best Practices für das Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool hängen vom Workload ab:

- Wenn Sie einen Tiering von primären FabricPool-Workload-Daten zu StorageGRID planen, sollten Sie sicherstellen, dass der FabricPool-Workload den Großteil der Bandbreite hat. Sie können eine Traffic-Klassifizierungsrichtlinie erstellen, um alle anderen Workloads einzuschränken.

  Im Allgemeinen sind FabricPool-Lesevorgänge wichtiger als Schreibvorgänge.

  Wenn beispielsweise andere S3-Clients dieses StorageGRID-System verwenden, sollten Sie eine Traffic-Klassifizierungsrichtlinie erstellen. Der Netzwerk-Traffic kann für die anderen Buckets, Mandanten, IP-Subnetze oder Load Balancer Endpunkte begrenzt werden.

- Im Allgemeinen sollten keine Grenzen für die Servicequalität für jeden FabricPool Workload gesetzt werden, sondern lediglich die anderen Workloads begrenzt werden.
- Die Einschränkungen, die für andere Workloads gelten, sollten das Verhalten dieser Workloads berücksichtigen. Die auferlegten Einschränkungen hängen auch von der Größe und den Funktionen des Grids und der erwarteten Auslastung ab.

Weitere Informationen: Verwalten von Richtlinien zur Verkehrsklassifizierung

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk Verkehrsklassifizierung**.
2. Geben Sie einen Namen und eine Beschreibung ein.

3. Erstellen Sie im Abschnitt Regeln für die Abgleich mindestens eine Regel.
   a. Wählen Sie **Erstellen**.
   b. Wählen Sie **Endpunkt** aus, und wählen Sie den für FabricPool erstellten Load Balancer-Endpunkt aus.

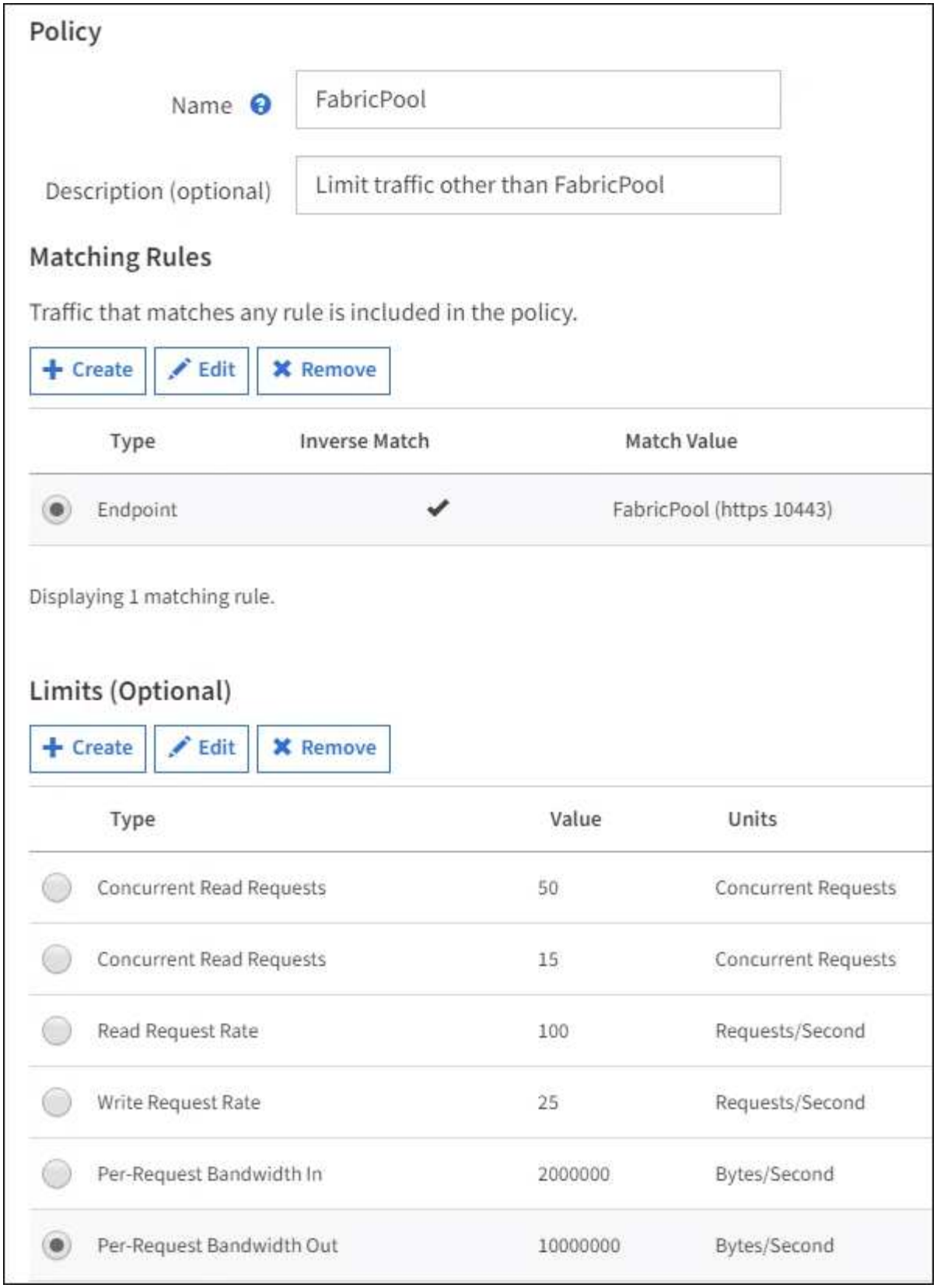
      Sie können auch das FabricPool-Mandantenkonto oder den Bucket auswählen.

   c. Wenn diese Verkehrsrichtlinie den Datenverkehr für die anderen Endpunkte einschränken soll, wählen Sie **Inverse Übereinstimmung**.
4. Optional können Sie eine oder mehrere Limits erstellen.

   Auch wenn für eine Traffic-Klassifizierungsrichtlinie keine Grenzen festgelegt sind, werden Kennzahlen erfasst, um Verkehrstrends zu verstehen.

   a. Wählen Sie **Erstellen**.
   b. Wählen Sie den zu begrenzenden Verkehrstyp und die anzuwählenden Grenzwerte aus.

      In diesem Beispiel zeigt die FabricPool Traffic-Klassifizierungsrichtlinie die Typen des zu begrenzenden Netzwerkverkehrs sowie die Arten von Werten an, die Sie auswählen können. Die Grenzwerte für eine tatsächliche Richtlinie basieren auf Ihren spezifischen Anforderungen.



5. Wählen Sie nach dem Erstellen der Traffic-Klassifizierungsrichtlinie die Richtlinie aus und wählen Sie dann **Metriken** aus, um festzustellen, ob die Richtlinie den Datenverkehr wie erwartet begrenzt.

Weitere Best Practices für StorageGRID und FabricPool

Wenn Sie ein StorageGRID-System für die Verwendung mit FabricPool konfigurieren, sollten Sie die Einstellung globaler Optionen vermeiden, die sich auf die Speicherung Ihrer Daten auswirken könnten.

Objektverschlüsselung

Bei der Konfiguration von StorageGRID können Sie optional die globale **gespeicherte Objektverschlüsselung**-Einstellung aktivieren, wenn für andere StorageGRID-Clients eine Datenverschlüsselung erforderlich ist (**KONFIGURATION System Grid-Optionen**). Die Daten, die von FabricPool zu StorageGRID verschoben werden, sind bereits verschlüsselt, d. h. die Aktivierung der StorageGRID-Einstellung ist nicht erforderlich. Die Client-seitige Verschlüsselung ist Eigentum von ONTAP.

Objektkomprimierung

Aktivieren Sie bei der Konfiguration von StorageGRID nicht die globale **Komprimierung gespeicherter Objekte**-Einstellung (**CONFIGURATION System Grid-Optionen**). Die Daten, die von FabricPool zu StorageGRID verschoben werden, werden bereits komprimiert. Durch das Aktivieren von **compress gespeicherter Objekte** wird die Größe eines Objekts nicht weiter verringert.

Konsistenzstufe

Für FabricPool Buckets ist die empfohlene Bucket-Konsistenzstufe **Read-after-New-write**, was die Standardeinstellung für einen neuen Bucket ist. Bearbeiten Sie FabricPool Buckets nicht, um **available** oder eine andere Konsistenzstufe zu verwenden.

FabricPool Tiering

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

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