



Konfigurieren Sie StorageGRID für FabricPool

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

- Konfigurieren Sie StorageGRID für FabricPool 1
 - StorageGRID für FabricPool wird konfiguriert 1
 - Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier 4
 - Informationslebenszyklus-Management von StorageGRID bei FabricPool-Daten ein 15
 - Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool. 18
 - Weitere Best Practices für StorageGRID und FabricPool 21

Konfigurieren Sie StorageGRID für FabricPool

Erfahren Sie, wie Sie StorageGRID als NetApp FabricPool Cloud Tier konfigurieren.

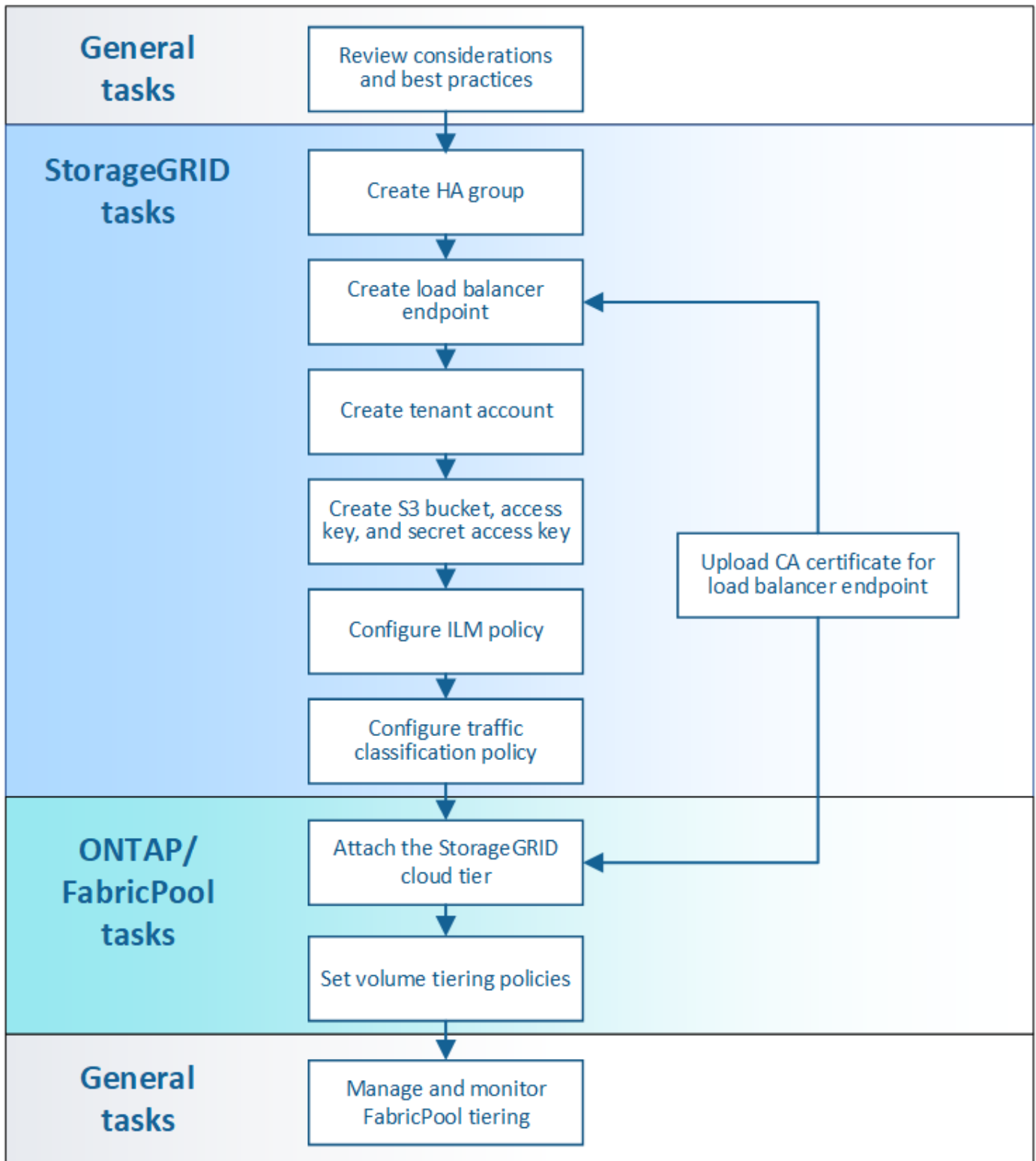
- ["StorageGRID für FabricPool wird konfiguriert"](#)
- ["Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier"](#)
- ["Informationslebenszyklus-Management von StorageGRID bei FabricPool-Daten ein"](#)
- ["Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool"](#)
- ["Weitere Best Practices für StorageGRID und FabricPool"](#)

StorageGRID für FabricPool wird konfiguriert

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

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.



Was Sie benötigen

Bevor Sie folgende Anweisungen verwenden:

- 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.

Verwandte Informationen

- ["TR-4598: FabricPool Best Practices für ONTAP 9.8"](#)
- ["ONTAP 9 Dokumentationszentrum"](#)

Was ist FabricPool

FabricPool ist eine ONTAP Hybrid-Storage-Lösung mit einem hochperformanten Flash-Aggregat als Performance-Tier und einem Objektspeicher als Cloud-Tier. Die Daten in einer FabricPool werden in einer Tier gespeichert, basierend darauf, ob häufig darauf zugegriffen wird oder nicht. Mit einer FabricPool senken Sie die Storage-Kosten, ohne dabei Einbußen bei Performance, Effizienz oder Sicherheit hinnehmen zu müssen.

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

Was ist Objekt-Storage

Objekt-Storage ist eine Storage-Architektur, die Daten als Objekte managt, anstatt anderer 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 enthalten.

Nutzung 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.

Verwendung mehrerer ONTAP Cluster mit StorageGRID

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.

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 für ONTAP 9.8"](#)
- ["ONTAP 9 Dokumentationszentrum"](#)

ONTAP Field	Beschreibung
Objektspeichername	Jeder eindeutige und beschreibende Name. Beispiel: StorageGRID_Cloud_Tier.
Anbietertyp	StorageGRID (System Manager) oder SGWS (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 Endpunkts für den Load Balancer für FabricPool"

ONTAP Field	Beschreibung
Servername	<p>Der vollständig qualifizierte Domänenname (FQDN) für den StorageGRID Load Balancer-Endpunkt. Beispiel: s3.storagegrid.company.com.</p> <p>Beachten Sie Folgendes:</p> <ul style="list-style-type: none"> • Der hier angegebene Domänenname muss mit dem Domännennamen 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. <p>"Konfigurieren des DNS-Servers für StorageGRID-IP-Adressen"</p>
Containername	<p>Der Name des StorageGRID-Buckets, den Sie mit diesem ONTAP-Cluster verwenden werden. Beispiel: fabricpool-bucket. Sie erstellen diesen Bucket im Tenant Manager.</p> <p>Beachten Sie Folgendes:</p> <ul style="list-style-type: none"> • 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. <p>"Erstellen eines S3-Buckets und Abrufen eines Zugriffsschlüssels"</p>
Zugriffsschlüssel und geheimes Passwort	<p>Der Zugriffsschlüssel und der geheime Zugriffsschlüssel für das StorageGRID-Mandantenkonto.</p> <p>Diese Werte generieren Sie im Tenant Manager.</p> <p>"Erstellen eines S3-Buckets und Abrufen eines Zugriffsschlüssels"</p>
SSL	<p>Muss aktiviert sein.</p>
Objektspeicherzertifikat	<p>Das CA-Zertifikat, das Sie beim Erstellen des StorageGRID Load Balancer-Endpunkts hochgeladen haben.</p> <p>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.</p> <p>"Erstellen eines Endpunkts für den Load Balancer für FabricPool"</p>

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, verwenden Sie den StorageGRID Grid-Manager, um mindestens einen Load Balancer-Endpunkt zu konfigurieren.

Was ist die Lastverteilung

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 bei Ihrem NetApp Ansprechpartner oder in den folgenden technischen Berichten:

"Optionen zum StorageGRID 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 einen Admin-Node und einen Gateway-Node oder sogar zwei Admin-Nodes enthalten. 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

Beim Erstellen eines Endpunkts für den Lastausgleich für die Verwendung mit FabricPool müssen Sie HTTPS als Protokoll verwenden. Sie können dann entweder ein Zertifikat hochladen, das entweder von einer öffentlich vertrauenswürdigen oder einer privaten Zertifizierungsstelle (CA) signiert ist, oder Sie können 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-Dienst herstellen, müssen Sie das Object Storage API Service Endpoints Server Certificate nicht hochladen.

Weitere Informationen zum Serverzertifikat für einen Lastausgleichsendpunkt:

- ["Managen des Lastausgleichs"](#)
- ["Härtungsrichtlinien für Serverzertifikate"](#)

Best Practices für Hochverfügbarkeitsgruppen

Bevor Sie StorageGRID als FabricPool Cloud-Tier anhängen, können Sie mithilfe von StorageGRID Grid Manager eine HA-Gruppe (High Availability, Hochverfügbarkeit) konfigurieren.

Eine HA-Gruppe (High Availability, Hochverfügbarkeit) ist das

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 allen Admin-Nodes besteht, hochverfügbaren Zugriff auf einige Management-Services für Admin-Nodes und den Load-Balancer-Service. Eine HA-Gruppe, die aus nur Gateway-Nodes oder Admin-Nodes und Gateway-Nodes besteht, bietet hochverfügbaren Zugriff auf den Shared Load Balancer Service.

Beim Erstellen einer HA-Gruppe wählen Sie Netzwerkschnittstellen aus, die zum Grid Network (eth0) oder dem Client-Netzwerk (eth2) gehören. Alle Schnittstellen in einer HA-Gruppe müssen sich im selben Netzwerk-Subnetz befinden.

Eine HA-Gruppe behält eine oder mehrere virtuelle IP-Adressen bei, die der aktiven Schnittstelle in der Gruppe hinzugefügt werden. Wenn die aktive Schnittstelle nicht mehr verfügbar ist, werden die virtuellen IP-Adressen in eine andere Schnittstelle verschoben. 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 Sie eine HA-Gruppe mit Nodes für den Lastausgleich konfigurieren, stellt FabricPool eine Verbindung zu den virtuellen IP-Adressen dieser HA-Gruppe her.

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 Daten mit primären Workloads verwenden möchten, müssen Sie eine HA-Gruppe erstellen, die mindestens zwei Load-Balancing-Nodes umfasst, um eine Unterbrechung beim Datenabruf zu vermeiden.
- 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 des DNS-Servers 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 FabricPool eine Verbindung zum StorageGRID Load Balancer Service herstellen. Dabei wird die IP-Adresse eines Gateway Node oder eines Admin-Nodes verwendet.

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 müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über die Berechtigung Root Access verfügen.

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. Siehe "[Verwalten von Hochverfügbarkeitsgruppen](#)".

Schritte

1. Wählen Sie **Konfiguration > Netzwerkeinstellungen > Hochverfügbarkeitsgruppen**.
2. Wählen Sie eine oder mehrere der Netzwerkschnittstellen aus. Die Netzwerkschnittstellen müssen entweder im Grid Network (eth0) oder im Client Network (eth2) zum selben Subnetz gehören.
3. Weisen Sie einen Knoten als bevorzugter Master zu.

Der bevorzugte Master ist die aktive Schnittstelle, wenn kein Fehler auftritt, der dazu führt, dass die VIP-Adressen einer Backup-Schnittstelle neu zugewiesen werden.

4. Geben Sie bis zu zehn IPv4-Adressen für die HA-Gruppe ein.

Die Adressen müssen sich im IPv4-Subnetz befinden, das von allen Mitgliedschnittstellen gemeinsam genutzt wird.

Create High Availability Group

High Availability Group

Name

Description

Interfaces

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Select Interfaces

Node Name	Interface	IPv4 Subnet	Preferred Master
DC1-ADM1	eth0	10.96.98.0/23	<input checked="" type="radio"/>
DC1-G1	eth0	10.96.98.0/23	<input type="radio"/>

Displaying 2 interfaces.

Virtual IP Addresses

Virtual IP Subnet: 10.96.98.0/23. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1

+

Cancel

Save

Erstellen eines Endpunkts für den Load Balancer für FabricPool

Wenn Sie StorageGRID für die Verwendung mit FabricPool konfigurieren, konfigurieren Sie einen Endpunkt für den Load Balancer und laden das Endpoint-Zertifikat für den Load Balancer hoch, mit dem die Verbindung zwischen ONTAP und StorageGRID gesichert werden kann.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.
- Sie haben die folgenden Dateien:
 - Serverzertifikat: Die benutzerdefinierte Serverzertifikatdatei.
 - Server Certificate Private Key: Die private Schlüsseldatei des benutzerdefinierten Serverzertifikats.

- CA-Paket: Eine einzelne 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 > Netzwerkeinstellungen > Balancer-Endpunkte Laden**.

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

2. Wählen Sie **Endpunkt hinzufügen**.
3. Geben Sie die folgenden Informationen ein.

Feld	Beschreibung
Anzeigename	Einen beschreibenden Namen für den Endpunkt
Port	<p>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.</p> <p>Hinweis: Ports, die von anderen Netzdiensten verwendet werden, sind nicht zulässig. Siehe Liste der Anschlüsse, die für interne und externe Kommunikation verwendet werden:</p> <p>"Referenz für Netzwerk-Ports"</p> <p>Sie müssen diese Portnummer an ONTAP angeben, wenn Sie StorageGRID als FabricPool Cloud Tier anhängen.</p>
Protokoll	Muss HTTPS sein.

Feld	Beschreibung
Endpunktbindungsmodus	<p>Verwenden Sie die Global-Einstellung (empfohlen) oder beschränken Sie die Zugänglichkeit dieses Endpunkts auf einen der folgenden Elemente:</p> <ul style="list-style-type: none"> • Spezifische virtuelle Hochverfügbarkeits-IP-Adressen (VIPs). Verwenden Sie diese Auswahl nur, wenn ein deutlich höheres Maß an Isolierung von Workloads erforderlich ist. • Spezielle Netzwerkschnittstellen bestimmter Nodes.

4. Wählen Sie **Speichern**.

Das Dialogfeld Endpunkt bearbeiten wird angezeigt.

5. Wählen Sie für * Endpoint Service Type* **S3** aus.

6. Wählen Sie **Zertifikat hochladen** (empfohlen) und navigieren Sie anschließend zu Ihrem Serverzertifikat, Ihrem privaten Zertifikatschlüssel und dem CA-Paket.

Load Certificate

Upload the PEM-encoded custom certificate, private key, and CA bundle files.

Server Certificate

Certificate Private Key

CA Bundle

7. Wählen Sie **Speichern**.

Erstellen eines Mandantenkontos für FabricPool

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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 Sie kein SSO verwenden, befolgen Sie die Anweisungen für "[Erstellen eines Mandantenkontos, wenn StorageGRID kein SSO verwendet](#)".

Schritte

1. Wählen Sie **Mieter**.
2. Wählen Sie **Erstellen**.
3. Geben Sie einen Anzeigenamen für das FabricPool-Mandantenkonto ein.
4. Wählen Sie **S3**.
5. Lassen Sie das Kontrollkästchen **Plattformdienste zulassen** aktiviert, um die Nutzung von Plattformdiensten zu aktivieren.

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

6. Lassen Sie das Feld **Storage Quota** leer.
7. Wählen Sie im Feld **Root Access Group** eine vorhandene föderierte Gruppe aus dem Grid Manager aus, um die ursprüngliche Root Access-Berechtigung für den Mandanten zu erhalten.
8. Wählen Sie **Speichern**.

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 müssen ein Mandantenkonto für die Nutzung von FabricPool erstellt haben.

Über diese Aufgabe

In diesen Anweisungen wird die Verwendung von StorageGRID Mandanten-Manager zur Erstellung eines Buckets beschrieben und Zugriffsschlüssel erhalten. Sie können diese Aufgaben auch mit der Mandantenmanagement-API oder der StorageGRID S3 REST-API ausführen.

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.

- Wählen Sie **STORAGE (S3) > Buckets** aus.
- Wählen Sie **Eimer erstellen**.
- 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.
- Wählen Sie die Region für diesen Bucket aus.

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

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name 

Region 

Cancel

Create bucket

- a. Wählen Sie **Eimer erstellen**.
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.

Informationslebenszyklus-Management von StorageGRID bei FabricPool-Daten ein

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.

Weitere Informationen: "[Objektmanagement mit ILM](#)"

ILM-Richtlinien für FabricPool-Daten

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. Bei Erasure Coding erfolgt eine höhere CPU-Auslastung, allerdings deutlich weniger Storage-Kapazität als mit Replizierung. Die Schemata 4+1 und 6+1 benötigen weniger Kapazität als 2+1, aber zu den Kosten eines niedrigeren Durchsatzes und weniger Flexibilität, wenn Sie Storage-Nodes während der Grid-Erweiterung hinzufügen.

- 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 den ILM-Regeln können FabricPool-Daten nicht mithilfe eines Archivierungs-Nodes auf Band archiviert werden, oder es kann ein Cloud-Storage-Pool zum Verschieben von FabricPool-Daten auf Glacier verwendet werden.



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: ["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	<code>fabricpool-bucket</code> Sie könnten auch nach dem FabricPool-Mandantenkonto filtern.
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	<i>None</i>
Erweiterte Filterung	<i>None</i>
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 handeln.
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 müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über die Berechtigung Root Access verfügen.

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 für andere Workloads gesetzten Grenzen müssen möglicherweise weit sein, um das unbekannt Verhalten dieser Workloads zu berücksichtigen. Die auferlegten Einschränkungen hängen auch von der Größe und den Funktionen des Grids und der erwarteten Auslastung ab.

Weitere Informationen: "[Verwalten von Richtlinien für die Verkehrsklassifizierung](#)"

Schritte

1. Wählen Sie **Konfiguration > Netzwerkeinstellungen > 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 FabricPool werden die Typen des Netzwerkdatenverkehrs, den Sie begrenzen können, sowie die Arten von Werten aufgeführt, die Sie auswählen können. Die Traffic-Typen und -Werte für eine tatsächliche Richtlinie basieren auf Ihren spezifischen Anforderungen.

Edit Traffic Classification Policy "FabricPool"

Policy

Name  FabricPool

Description (optional) Limit traffic other than FabricPool

Matching Rules

Traffic that matches any rule is included in the policy.

 Create  Edit  Remove

	Type	Inverse Match	Match Value
<input type="radio"/>	Endpoint	<input checked="" type="checkbox"/>	FabricPool (https 10443)

Displaying 1 matching rule.

Limits (Optional)

 Create  Edit  Remove

	Type	Value	Units
<input type="radio"/>	Concurrent Read Requests	50	Concurrent Requests
<input type="radio"/>	Concurrent Write Requests	15	Concurrent Requests
<input type="radio"/>	Read Request Rate	100	Requests/Second
<input type="radio"/>	Write Request Rate	25	Requests/Second
<input type="radio"/>	Per-Request Bandwidth In	2000000	Bytes/Second
<input type="radio"/>	Per-Request Bandwidth Out	10000000	Bytes/Second

Displaying 6 limits.

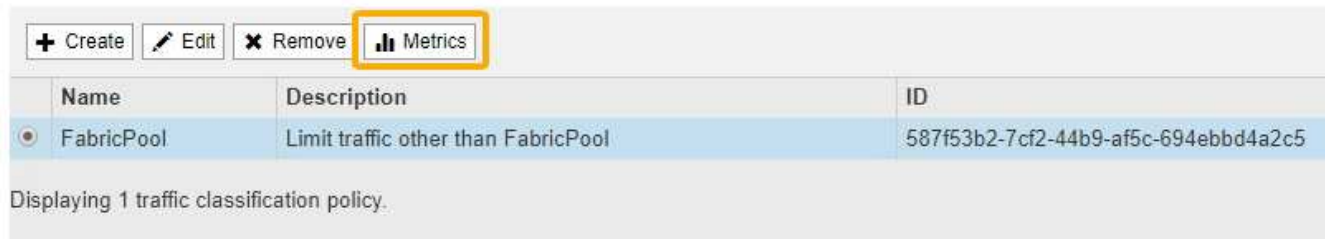
Cancel

Save

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.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.



Name	Description	ID
<input checked="" type="radio"/> FabricPool	Limit traffic other than FabricPool	587f53b2-7cf2-44b9-af5c-694ebbd4a2c5

Displaying 1 traffic classification policy.

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 > Systemeinstellungen > Rasteroptionen**). 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 (**Konfiguration > Systemeinstellungen > Rasteroptionen**). 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 AFF 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.

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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