Konfigurieren Sie StorageGRID manuell

StorageGRID 11.8

NetApp
May 17, 2024

Inhalt

Konfigurieren Sie StorageGRID manuell

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 ist eine Sammlung von Nodes, die jeweils den StorageGRID Lastausgleich enthalten. Eine HA-Gruppe kann Gateway-Nodes, Admin-Nodes oder beides enthalten.

Sie können eine HA-Gruppe verwenden, um FabricPool-Datenverbindungen verfügbar zu halten. Eine HA-Gruppe verwendet virtuelle IP-Adressen (VIPs), um hochverfügbaren Zugriff auf den Load Balancer-Service zu ermöglichen. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload mit geringen Auswirkungen auf den FabricPool-Betrieb managen.

Weitere Informationen zu dieser Aufgabe finden Sie unter "Management von Hochverfügbarkeitsgruppen". Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu "Öffnen und Abschließen des FabricPool Setup-Assistenten".

Bevor Sie beginnen

- Sie haben die geprüft "Best Practices für Hochverfügbarkeitsgruppen ab".
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".
- Wenn Sie ein VLAN verwenden möchten, haben Sie die VLAN-Schnittstelle erstellt. Siehe "Konfigurieren Sie die VLAN-Schnittstellen".

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **High Availability groups**.
2. Wählen Sie **Erstellen**.
3. Füllen Sie für den Schritt **Enter Details** die folgenden Felder aus.

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

4. Wählen Sie im Schritt **Schnittstellen hinzufügen** die Knotenschnittstellen aus, die Sie in dieser HA-Gruppe verwenden möchten.

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

   Sie können einen oder mehrere Nodes auswählen, aber Sie können nur eine Schnittstelle für jeden Node auswählen.

5. Bestimmen Sie für den Schritt **priorisiere Schnittstellen** die primäre Schnittstelle und alle Backup-Schnittstellen für diese HA-Gruppe.

   Ziehen Sie Zeilen, 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, werden die virtuellen IP-Adressen (VIP-Adressen) zur ersten Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. 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. Füllen Sie für den Schritt **IP-Adressen eingeben** die folgenden Felder aus.

Feld	Beschreibung
Subnetz-CIDR	Die Adresse des VIP-Subnetzes in CIDR Notation—eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetz-Länge (0-32). Die Netzwerkadresse darf keine Host-Bits festgelegt haben. Beispiel: `192.16.0.0/22`.
Gateway-IP-Adresse (optional)	Optional Wenn sich die ONTAP-IP-Adressen, die für den Zugriff auf StorageGRID verwendet werden, nicht im selben Subnetz wie die StorageGRID-VIP-Adressen befinden, geben Sie die IP-Adresse des lokalen StorageGRID-VIP-Gateways ein. Die IP-Adresse des lokalen Gateways muss sich im VIP-Subnetz befinden.
Virtuelle IP-Adresse	Geben Sie mindestens eine und nicht mehr als 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 weitere IPv4- und IPv6-Adressen angeben.

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

Erstellen eines Load Balancer-Endpunkts für FabricPool

StorageGRID verwendet einen Load Balancer zum Managen des Workloads von Client-Applikationen wie FabricPool. Load Balancing maximiert Geschwindigkeit und Verbindungskapazität über mehrere Storage Nodes hinweg.

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

Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu "Öffnen und Abschließen des FabricPool Setup-Assistenten".

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".
- Sie haben den General überprüft "Überlegungen zum Lastausgleich" Sowie dem "Best Practices für Lastausgleich für FabricPool".

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **Load Balancer Endpunkte**.
2. Wählen Sie **Erstellen**.
3. Füllen Sie für den Schritt **Enter Endpoint Details** die folgenden Felder aus.

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt.
Port	Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist für den ersten erstellten Endpunkt standardmäßig auf 10433 eingestellt, Sie können jedoch jeden nicht verwendeten externen Port eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Nodes konfiguriert. Diese Ports sind für Admin-Nodes reserviert. **Hinweis:** von anderen Netzdiensten verwendete Ports sind nicht erlaubt. Siehe "Referenz für Netzwerk-Ports". Sie geben diese Nummer an ONTAP an, wenn Sie StorageGRID als FabricPool-Cloud-Tier hinzufügen.
Client-Typ	Wählen Sie **S3**.
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 der Zugriff auf den Endpunkt über eine beliebige IP-Adresse oder über spezifische IP-Adressen und Netzwerkschnittstellen erfolgt.

Modus	Beschreibung
Global (Standard)	Clients können über die IP-Adresse eines beliebigen Gateway-Node oder Admin-Node, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie die **Global**-Einstellung (Standard), es sei denn, Sie müssen die Zugriffsmöglichkeiten dieses Endpunkts einschränken.

Modus	Beschreibung
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überlappen.
Node-Schnittstellen	Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Node-Typ	Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.

5. Wählen Sie für den Schritt **Tenant Access** eine der folgenden Optionen aus:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen. **Alle Mandanten zulassen** ist fast immer die geeignete Option für den für FabricPool verwendeten Load Balancer Endpunkt. Sie müssen diese Option auswählen, wenn Sie noch keine Mandantenkonten erstellt haben.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt für den Zugriff auf ihre Buckets verwenden.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Dieser Endpunkt kann von allen anderen Mandanten verwendet werden.

6. Wählen Sie für den Schritt **Zertifikat anhängen** eine der folgenden Optionen aus:

Feld	Beschreibung
Zertifikat hochladen (empfohlen)	Verwenden Sie diese Option, um ein CA-signiertes Serverzertifikat, einen privaten Zertifikatschlüssel und ein optionales CA-Paket hochzuladen.
Zertifikat wird generiert	Verwenden Sie diese Option, um ein selbstsigniertes Zertifikat zu generieren. Siehe "Konfigurieren von Load Balancer-Endpunkten" Für Details, was eingegeben werden soll.

Feld	Beschreibung
StorageGRID S3 und Swift-Zertifikat verwenden	Diese Option ist nur verfügbar, wenn Sie bereits eine benutzerdefinierte Version des globalen StorageGRID-Zertifikats hochgeladen oder generiert haben. Siehe "Konfigurieren von S3- und Swift-API-Zertifikaten" Entsprechende Details.

7. 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.

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.

Weitere Informationen zu dieser Aufgabe finden Sie unter "Erstellen eines Mandantenkontos". Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu "Öffnen und Abschließen des FabricPool Setup-Assistenten".

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".

Schritte

1. Wählen Sie **MIETER**.
2. Wählen Sie **Erstellen**.
3. Geben Sie für die Schritte zum Eingeben von Details die folgenden Informationen ein.

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 Mandanten.
Client-Typ	Muss **S3** für FabricPool sein.
Storage-Kontingent (optional)	Lassen Sie dieses Feld für FabricPool leer.

4. Für den Schritt Berechtigungen auswählen:
   a. Wählen Sie nicht **Plattformdienste zulassen**.

FabricPool Mandanten benötigen in der Regel keine Plattform-Services, wie z. B. CloudMirror-Replizierung.

b. Wählen Sie optional **eigene Identitätsquelle verwenden**.

c. Wählen Sie nicht **S3 Select zulassen**.

FabricPool-Mandanten müssen in der Regel nicht S3 Select verwenden.

d. Wählen Sie optional **Grid Federation Connection** verwenden, um dem Mandanten die Verwendung eines zu ermöglichen "Netzverbundverbindung" Für Account-Klonen und Grid-übergreifende Replizierung. Wählen Sie dann die zu verwendende Netzverbundverbindung aus.

5. Geben Sie für den Schritt Root-Zugriff definieren an, welcher Benutzer die anfängliche Root-Zugriffsberechtigung für das Mandantenkonto erhält, je nachdem, ob das StorageGRID-System verwendet "Identitätsföderation", "Single Sign On (SSO)"Oder beides.

Option	Tun Sie das
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. b. Geben Sie optional das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. Keine lokalen Benutzer können sich anmelden.

6. Wählen Sie **Create Tenant**.

Erstellen eines S3-Buckets und Abrufen von Zugriffsschlüsseln

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.

Weitere Informationen zu dieser Aufgabe finden Sie unter "S3-Bucket erstellen" Und "Erstellen Ihrer eigenen S3-Zugriffsschlüssel". Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu "Öffnen und Abschließen des FabricPool Setup-Assistenten".

Bevor Sie beginnen

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

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 **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3)** > **Buckets**.
   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.

   d. Wählen Sie die Region für diesen Bucket aus.

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

   e. Wählen Sie **Weiter**.
   f. Wählen Sie **Eimer erstellen**.

      Wählen Sie nicht **enable object Versioning** für den FabricPool Bucket aus. Bearbeiten Sie einen FabricPool-Bucket nicht, um **verfügbar** oder eine nicht standardmäßige Konsistenz zu verwenden. Die empfohlene Bucket-Konsistenz für FabricPool-Buckets ist **Read-after-New-write**, was die Standardkonsistenz für einen neuen Bucket ist.

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 in StorageGRID einen neuen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel generieren, geben Sie die neuen Schlüssel in ONTAP ein, bevor Sie die alten Werte aus StorageGRID löschen. Andernfalls könnte ONTAP vorübergehend seinen Zugriff auf StorageGRID verlieren.

Konfigurieren Sie ILM für FabricPool-Daten

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

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. Simulieren Sie vor der Aktivierung einer neuen Richtlinie, um zu bestätigen, dass sie so funktioniert, wie sie zum Schutz von Inhalten vor Verlust vorgesehen ist. Weitere Informationen finden Sie unter "Objektmanagement mit ILM".

> Verwenden Sie zur Vermeidung von Datenverlust keine ILM-Regel, die ausläuft oder die Cloud-Tiering-Daten von FabricPool löscht. Setzen Sie die Aufbewahrungsfrist auf **Forever**, um sicherzustellen, dass FabricPool-Objekte nicht durch StorageGRID ILM gelöscht werden.

Bevor Sie beginnen

- Sie haben die geprüft "Best Practices für die Verwendung von ILM mit FabricPool-Daten".
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "ILM oder Root-Zugriffsberechtigung".
- Wenn Sie von einer früheren StorageGRID-Version auf StorageGRID 11.8 aktualisiert haben, haben Sie den zu verwendenden Speicherpool konfiguriert. Im Allgemeinen sollten Sie für jeden StorageGRID-Standort, den Sie zum Speichern von Daten verwenden, einen Speicherpool erstellen.

  > Diese Voraussetzung gilt nicht, wenn Sie zunächst StorageGRID 11.7 oder 11.8 installiert haben. Wenn Sie eine dieser Versionen zuerst installieren, werden Speicherpools automatisch für jeden Standort erstellt.

Schritte

1. 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 + 1 Erasure Coding für FabricPool-Daten
Bucket-Name	`fabricpool-bucket` Sie könnten auch nach dem FabricPool-Mandantenkonto filtern.
Erweiterte Filter	Objektgröße größer als 0.2 MB. **Hinweis:** FabricPool schreibt nur 4 MB Objekte, aber Sie müssen einen Objektgrößenfilter hinzufügen, da diese Regel Erasure Coding verwendet.

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Zeitraum und Platzierungen	Ab Tag 0 für immer speichern Speichern Sie Objekte durch Erasure Coding mit dem 2+1-EC-Schema in Denver und bewahren Sie diese Objekte für immer in StorageGRID auf. Verwenden Sie zur Vermeidung von Datenverlust keine ILM-Regel, die ausläuft oder die Cloud-Tiering-Daten von FabricPool löscht.
Aufnahmeverhalten	Ausgeglichen

2. Erstellen Sie eine standardmäßige ILM-Regel, die zwei replizierte Kopien von Objekten erstellt, die der ersten Regel nicht zugeordnet sind. Wählen Sie keinen einfachen Filter (Mandantenkonto oder Bucket-Name) oder keine erweiterten Filter aus.

Regeldefinition	Beispielwert
Regelname	Zwei replizierte Kopien
Bucket-Name	*None*
Erweiterte Filter	*None*
Referenzzeit	Aufnahmezeit
Zeitraum und Platzierungen	Ab Tag 0 für immer speichern Speichern Sie Objekte, indem Sie 2 Kopien in Denver replizieren.
Aufnahmeverhalten	Ausgeglichen

3. Erstellen Sie eine ILM-Richtlinie und wählen Sie die beiden Regeln aus. Da die Replikationsregel keine Filter verwendet, kann es sich um die Standardregel (letzte) für die Richtlinie handelt.
4. Aufnahme von Testobjekten in das Raster
5. Simulieren Sie die Richtlinie mit den Testobjekten, um das Verhalten zu überprüfen.
6. Aktivieren Sie die Richtlinie.

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

- Die Daten-Tiering von FabricPool in `fabricpool-bucket` Erasure Coding wird mit dem 2+1 Erasure Coding Verfahren durchgeführt. 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 Kopien werden für immer in StorageGRID aufbewahrt. StorageGRID ILM wird diese Objekte nicht löschen.

Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool

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

Weitere Informationen zu dieser Aufgabe finden Sie unter "Verwalten von Richtlinien zur Verkehrsklassifizierung". Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu "Öffnen und Abschließen des FabricPool Setup-Assistenten".

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".

Über diese Aufgabe

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

- Bei der Planung, primäre FabricPool Workload-Daten auf StorageGRID zu verschieben, sollte sichergestellt werden, dass der FabricPool-Workload den größten Teil 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 Sie keine Quality of Service-Limits für FabricPool-Workloads einführen; Sie sollten nur die anderen Workloads begrenzen.

- 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.

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **traffic classification**.
2. Wählen Sie **Erstellen**.
3. Geben Sie einen Namen und eine Beschreibung (optional) für die Richtlinie ein und wählen Sie **Weiter**.
4. Fügen Sie für den Schritt übereinstimmende Regeln hinzufügen mindestens eine Regel hinzu.
   a. Wählen Sie **Regel hinzufügen**
   b. Wählen Sie unter Typ * Load Balancer Endpunkt* aus, und wählen Sie den Load Balancer Endpunkt aus, den Sie für FabricPool erstellt haben.

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

c. Wenn diese Datenverkehrsrichtlinie den Datenverkehr für die anderen Endpunkte einschränken soll, wählen Sie **inverse Übereinstimmung**.

5. Fügen Sie optional eine oder mehrere Grenzwerte hinzu, um den Netzwerkverkehr zu steuern, der der Regel entspricht.

> StorageGRID sammelt Kennzahlen, auch wenn Sie keine Limits hinzufügen, sodass Sie Verkehrstrends besser verstehen können.

a. Wählen Sie **Limit hinzufügen**.

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

6. Wählen Sie **Weiter**.

7. Lesen und prüfen Sie die Richtlinie zur Verkehrsklassifizierung. Verwenden Sie die Schaltfläche * Zurück*, um zurückzugehen und Änderungen vorzunehmen. Wenn Sie mit der Richtlinie zufrieden sind, wählen Sie **Speichern und fortfahren**.

Nach dem Ende

"Zeigen Sie Metriken zum Netzwerkverkehr an" Um zu überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzwerte durchsetzen.