Managen Sie den Lastausgleich

StorageGRID 11.8

NetApp
May 10, 2024

Inhalt

Managen Sie den Lastausgleich

Überlegungen zum Lastausgleich

Mit Lastausgleich können Workloads bei der Aufnahme und dem Abruf von S3 und Swift Clients genutzt werden.

Was ist Load Balancing?

Wenn eine Client-Applikation Daten eines StorageGRID Systems speichert oder abruft, verwendet StorageGRID einen Load Balancer, um den Aufnahme- und Abruf-Workload zu managen. Load Balancing maximiert die Geschwindigkeit und die Verbindungskapazität, indem der 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".

Wie viele Nodes für Lastausgleich benötige ich?

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. Stellen Sie sicher, dass für jeden Load Balancing-Node eine geeignete Netzwerk-, Hardware- oder Virtualisierungsinfrastruktur bereitgestellt wird, unabhängig davon, ob Sie Services-Appliances, Bare-Metal-Nodes oder VM-basierte Nodes nutzen.

Was ist ein Endpunkt eines Load Balancers?

Ein Load Balancer-Endpunkt definiert den Port und das Netzwerkprotokoll (HTTPS oder HTTP), über das eingehende und ausgehende Client-Anwendungsanforderungen auf die Knoten zugreifen, die den Load Balancer-Dienst enthalten. Der Endpunkt definiert außerdem den Client-Typ (S3 oder Swift), den Bindungsmodus und optional eine Liste zulässiger oder blockierter Mandanten.

Um einen Load Balancer-Endpunkt zu erstellen, wählen Sie entweder **CONFIGURATION** > **Network** > **Load Balancer-Endpunkte** oder schließen Sie den FabricPool- und S3-Setup-Assistenten ab. Weitere Informationen:

- "Konfigurieren von Load Balancer-Endpunkten"
- "Verwenden Sie den S3-Einrichtungsassistenten"
- "Verwenden Sie den FabricPool-Einrichtungsassistenten"

Überlegungen zum Port

Der Port für einen Load Balancer-Endpunkt ist für den ersten erstellten Endpunkt standardmäßig auf 10433 gesetzt. Sie können jedoch einen beliebigen nicht verwendeten externen Port zwischen 1 und 65535 angeben. Wenn Sie Port 80 oder 443 verwenden, verwendet der Endpunkt nur den Load Balancer-Dienst auf Gateway-Nodes. Diese Ports sind für Admin-Nodes reserviert. Wenn Sie denselben Port für mehr als einen Endpunkt verwenden, müssen Sie für jeden Endpunkt einen anderen Bindungsmodus angeben.

Von anderen Netzdiensten verwendete Ports sind nicht zulässig. Siehe "Referenz für Netzwerk-Ports".

Überlegungen zum Netzwerkprotokoll

In den meisten Fällen sollte für die Verbindungen zwischen Client-Anwendungen und StorageGRID die TLS-Verschlüsselung (Transport Layer Security) verwendet werden. Eine Verbindung mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen, insbesondere in Produktionsumgebungen. Wenn Sie das Netzwerkprotokoll für den StorageGRID Load Balancer-Endpunkt auswählen, sollten Sie **HTTPS** auswählen.

Überlegungen für Load Balancer-Endpunktzertifikate

Wenn Sie **HTTPS** als Netzwerkprotokoll für den Load Balancer-Endpunkt auswählen, müssen Sie ein Sicherheitszertifikat angeben. Beim Erstellen des Load Balancer-Endpunkts können Sie eine der folgenden drei Optionen verwenden:

- **Laden Sie ein signiertes Zertifikat hoch (empfohlen)**. Dieses Zertifikat kann entweder von einer öffentlich vertrauenswürdigen oder einer privaten Zertifizierungsstelle (CA) signiert werden. Die Verwendung eines öffentlich vertrauenswürdigen CA-Serverzertifikats zum Sichern der Verbindung ist die beste Methode. Im Gegensatz zu generierten Zertifikaten können von einer CA signierte Zertifikate unterbrechungsfrei gedreht werden, was dazu beitragen kann, Ablaufprobleme zu vermeiden.

  Sie müssen die folgenden Dateien abrufen, bevor Sie den Load Balancer-Endpunkt erstellen:

  - Die Zertifikatdatei des benutzerdefinierten Servers.
  - Die Datei mit dem privaten Schlüssel des benutzerdefinierten Serverzertifikats.
  - Optional ein CA-Bündel der Zertifikate jeder zwischengeschalteten Zertifizierungsstelle.
- **Generieren Sie ein selbst signiertes Zertifikat**.
- **Verwenden Sie das globale StorageGRID S3 und Swift Zertifikat**. Sie müssen eine benutzerdefinierte Version dieses Zertifikats hochladen oder generieren, bevor Sie es für den Load Balancer-Endpunkt auswählen können. Siehe "Konfigurieren von S3- und Swift-API-Zertifikaten".

Welche Werte brauche ich?

Zum Erstellen des Zertifikats müssen Sie alle Domänennamen und IP-Adressen kennen, die von S3- oder Swift-Client-Anwendungen für den Zugriff auf den Endpunkt verwendet werden.

Der Eintrag **Subject DN** (Distinguished Name) für das Zertifikat muss den vollständig qualifizierten Domänennamen enthalten, den die Client-Anwendung für StorageGRID verwendet. Beispiel:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Bei Bedarf kann das Zertifikat Platzhalter verwenden, um die vollständig qualifizierten Domänennamen aller Admin-Nodes und Gateway-Nodes darzustellen, auf denen der Load Balancer-Dienst ausgeführt wird. Beispiel: `*.storagegrid.example.com` Verwendet den Platzhalter * für die Darstellung `adm1.storagegrid.example.com` Und `gn1.storagegrid.example.com`.

Wenn Sie S3 Virtual Hosted-Style-Anfragen verwenden möchten, muss das Zertifikat für jeden Eintrag auch einen **Alternative Name**-Eintrag enthalten "Der Domänenname des S3-Endpunkts" Sie haben konfiguriert, einschließlich aller Platzhalternamen. Beispiel:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

Wenn Sie Platzhalter für Domänennamen verwenden, lesen Sie die "Härtungsrichtlinien für Serverzertifikate".

Außerdem müssen Sie für jeden Namen im Sicherheitszertifikat einen DNS-Eintrag definieren.

Wie verwalte ich auslaufende Zertifikate?

Wenn das Zertifikat, mit dem die Verbindung zwischen der S3-Anwendung und StorageGRID gesichert wird, abläuft, kann die Applikation möglicherweise vorübergehend den Zugriff auf StorageGRID verlieren.

Befolgen Sie die folgenden Best Practices, um Probleme mit dem Ablauf von Zertifikaten zu vermeiden:

- Überwachen Sie sorgfältig alle Warnungen, die darauf hinweisen, dass sich das Ablaufdatum des Zertifikats nähert, z. B. das Endpunktzertifikat **Ablauf des Load Balancer** und **Ablauf des globalen Serverzertifikats für S3- und Swift-API**-Warnungen.
- Halten Sie die Versionen des Zertifikats für die StorageGRID- und S3-Anwendung immer synchron. Wenn Sie das für einen Load Balancer-Endpunkt verwendete Zertifikat ersetzen oder erneuern, müssen Sie das von der S3-Anwendung verwendete entsprechende Zertifikat ersetzen oder erneuern.
- Ein öffentlich signiertes CA-Zertifikat verwenden. Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat verwenden, können Sie bald abgelaufene Zertifikate unterbrechungsfrei ersetzen.
- Wenn Sie ein selbstsigniertes StorageGRID-Zertifikat generiert haben und dieses Zertifikat kurz vor dem Ablauf steht, müssen Sie das Zertifikat sowohl in StorageGRID als auch in der S3-Anwendung manuell ersetzen, bevor das vorhandene Zertifikat abläuft.

Überlegungen zum Bindungsmodus

Im Bindungsmodus können Sie festlegen, welche IP-Adressen für den Zugriff auf einen Load Balancer-Endpunkt verwendet werden können. Wenn ein Endpunkt einen Bindungsmodus verwendet, können Clientanwendungen nur auf den Endpunkt zugreifen, wenn sie eine zulässige IP-Adresse oder den entsprechenden vollständig qualifizierten Domänennamen (FQDN) verwenden. Client-Anwendungen, die eine andere IP-Adresse oder FQDN verwenden, können nicht auf den Endpunkt zugreifen.

Sie können einen der folgenden Bindungsmodi festlegen:

- **Global** (Standard): Client-Anwendungen können über die IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, die virtuelle IP-Adresse (VIP) einer HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie diese Einstellung, es sei denn, Sie müssen den Zugriff auf einen Endpunkt einschränken.

- **Virtuelle IPs von HA-Gruppen**. Client-Anwendungen müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden.
- **Knotenschnittstellen**. Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden.
- **Knotentyp**. 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.

Überlegungen für den Mandantenzugriff

Der Mandantenzugriff ist eine optionale Sicherheitsfunktion, mit der Sie steuern können, welche StorageGRID-Mandantenkonten einen Load-Balancer-Endpunkt für den Zugriff auf ihre Buckets verwenden können. Sie können allen Mandanten den Zugriff auf einen Endpunkt erlauben (Standard), oder Sie können eine Liste der zulässigen oder blockierten Mandanten für jeden Endpunkt festlegen.

Sie können diese Funktion nutzen, um eine bessere Sicherheitsisolierung zwischen Mandanten und ihren Endpunkten zu ermöglichen. Mit dieser Funktion können Sie beispielsweise sicherstellen, dass die streng geheimen oder streng klassifizierten Materialien eines Mandanten für andere Mieter nicht zugänglich sind.

> Für die Zugriffssteuerung wird der Mandant aus den Zugriffsschlüsseln ermittelt, die in der Client-Anfrage verwendet werden. Wenn im Rahmen der Anfrage keine Zugriffsschlüssel angegeben werden (z. B. mit anonymem Zugriff), wird der Bucket-Eigentümer zur Ermittlung des Mandanten verwendet.

Beispiel für Mandantenzugriff

Um zu verstehen, wie diese Sicherheitsfunktion funktioniert, betrachten Sie das folgende Beispiel:

1. Sie haben zwei Lastausgleichsendpunkte wie folgt erstellt:
   - **Öffentlicher** Endpunkt: Nutzt Port 10443 und erlaubt den Zugriff auf alle Mandanten.
   - **Top secret** Endpunkt: Verwendet Port 10444 und erlaubt nur den Zugriff auf den **Top secret** Mieter. Alle anderen Mandanten werden für den Zugriff auf diesen Endpunkt gesperrt.
2. Der `top-secret.pdf` Befindet sich in einem Eimer im Besitz des **Top Secret** Mieters.

Um auf den zuzugreifen `top-secret.pdf`Ein Benutzer im **`Top Secret`**-Mieter kann eine GET-Anfrage an ausstellen `\https://w.x.y.z:10444/top-secret.pdf`. Da dieser Mandant den Endpunkt 10444 verwenden darf, kann der Benutzer auf das Objekt zugreifen. Wenn ein Benutzer eines anderen Mandanten jedoch dieselbe Anforderung an dieselbe URL ausgibt, erhält er eine Meldung über „Zugriff verweigert“. Der Zugriff wird verweigert, selbst wenn die Anmeldeinformationen und die Signatur gültig sind.

CPU-Verfügbarkeit

Der Load Balancer Service läuft auf jedem Admin-Node und Gateway-Node unabhängig, wenn der S3- oder Swift-Datenverkehr zu den Storage-Nodes weitergeleitet wird. Durch eine Gewichtung leitet der Load Balancer-Service mehr Anfragen an Storage-Nodes mit höherer CPU-Verfügbarkeit weiter. Die Informationen zur CPU-Auslastung des Knotens werden alle paar Minuten aktualisiert. Die Gewichtung kann jedoch häufiger aktualisiert werden. Allen Storage-Nodes wird ein Mindestwert für das Basisgewicht zugewiesen, selbst wenn ein Node eine Auslastung von 100 % meldet oder seine Auslastung nicht meldet.

In manchen Fällen sind die Informationen zur CPU-Verfügbarkeit auf den Standort beschränkt, an dem sich

der Load Balancer Service befindet.

Konfigurieren von Load Balancer-Endpunkten

Load Balancer-Endpunkte bestimmen die Ports und Netzwerkprotokolle S3 und Swift-Clients können beim Herstellen einer Verbindung zum StorageGRID Load Balancer auf Gateway und Admin-Nodes verwendet werden. Sie können Endpunkte auch für den Zugriff auf Grid Manager, Tenant Manager oder beide verwenden.

> Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".
- Sie haben die geprüft "Überlegungen zum Lastausgleich".
- Wenn Sie zuvor einen Port neu zugeordnet haben, den Sie für den Load Balancer-Endpunkt verwenden möchten, haben Sie diesen "Port-Remap wurde entfernt".
- Sie haben alle Hochverfügbarkeitsgruppen (High Availability groups, die Sie verwenden möchten, erstellt. HA-Gruppen werden empfohlen, jedoch nicht erforderlich. Siehe "Management von Hochverfügbarkeitsgruppen".
- Wenn der Endpunkt des Load Balancer von verwendet wird "S3 Mandanten für S3 Select", Es darf die IP-Adressen oder FQDNs von Bare-Metal-Knoten nicht verwenden. Für die für S3 Select verwendeten Load Balancer-Endpunkte sind nur Service-Appliances und VMware-basierte Software-Nodes zulässig.
- Sie haben alle VLAN-Schnittstellen konfiguriert, die Sie verwenden möchten. Siehe "Konfigurieren Sie die VLAN-Schnittstellen".
- Wenn Sie einen HTTPS-Endpunkt erstellen (empfohlen), haben Sie die Informationen für das Serverzertifikat.

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

  - Zum Hochladen eines Zertifikats benötigen Sie das Serverzertifikat, den privaten Zertifikatschlüssel und optional ein CA-Bundle.
  - Zum Generieren eines Zertifikats benötigen Sie alle Domain-Namen und IP-Adressen, die S3- oder Swift-Clients für den Zugriff auf den Endpunkt verwenden. Sie müssen auch das Thema (Distinguished Name) kennen.
  - Wenn Sie das StorageGRID S3- und Swift-API-Zertifikat verwenden möchten (das auch für direkte Verbindungen zu Speicherknoten verwendet werden kann), haben Sie das Standardzertifikat bereits durch ein benutzerdefiniertes Zertifikat ersetzt, das von einer externen Zertifizierungsstelle signiert ist. Siehe "Konfigurieren von S3- und Swift-API-Zertifikaten".

Erstellen Sie einen Endpunkt für den Load Balancer

Jeder S3- oder Swift-Client-Load-Balancer-Endpunkt gibt einen Port, einen Client-Typ (S3 oder Swift) und ein Netzwerkprotokoll (HTTP oder HTTPS) an. Endpunkte für den Lastenausgleich der Verwaltungsschnittstelle geben einen Port, einen Schnittstellentyp und ein nicht vertrauenswürdiges Client-Netzwerk an.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **Load Balancer Endpunkte**.
2. Um einen Endpunkt für einen S3- oder Swift-Client zu erstellen, wählen Sie die Registerkarte **S3 oder Swift-Client** aus.
3. Um einen Endpunkt für den Zugriff auf Grid Manager, Tenant Manager oder beides zu erstellen, wählen Sie die Registerkarte **Verwaltungsschnittstelle** aus.
4. Wählen Sie **Erstellen**.

Geben Sie Details zu Endpunkten ein

Schritte

1. Wählen Sie die entsprechenden Anweisungen aus, um Details für den Typ des Endpunkts einzugeben, den Sie erstellen möchten.

S3- oder Swift-Client

Feld	Beschreibung
Name	Ein beschreibbarer Name für den Endpunkt, der in der Tabelle auf der Seite Load Balancer Endpunkte angezeigt wird.
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 zwischen 1 und 65535 eingeben. Wenn Sie **80** oder **8443** eingeben, wird der Endpunkt nur auf Gateway Nodes konfiguriert, es sei denn, Sie haben Port 8443 freigegeben. Anschließend können Sie Port 8443 als S3-Endpunkt verwenden, und der Port wird sowohl auf dem Gateway als auch auf den Admin-Nodes konfiguriert.
Client-Typ	Der Typ der Client-Anwendung, die diesen Endpunkt verwenden wird, entweder **S3** oder **Swift**.
Netzwerkprotokoll	Das Netzwerkprotokoll, das Clients bei der Verbindung mit diesem Endpunkt verwenden werden. • Wählen Sie **HTTPS** für sichere, TLS verschlüsselte Kommunikation (empfohlen). Sie müssen ein Sicherheitszertifikat anhängen, bevor Sie den Endpunkt speichern können. • Wählen Sie **HTTP** für eine weniger sichere, unverschlüsselte Kommunikation. Verwenden Sie HTTP nur für ein Grid, das nicht produktionsbereit ist.

Managementoberfläche

Feld	Beschreibung
Name	Ein beschreibbarer Name für den Endpunkt, der in der Tabelle auf der Seite Load Balancer Endpunkte angezeigt wird.
Port	Der StorageGRID-Port, über den Sie auf den Grid-Manager, den Mandantenmanager oder beide zugreifen möchten. • Grid Manager: **8443** • Mieter-Manager: **9443** • Grid Manager und Tenant Manager: **443** **Hinweis**: Sie können diese voreingestellten Ports oder andere verfügbare Ports verwenden.
Schnittstellentyp	Aktivieren Sie das Optionsfeld für die StorageGRID-Schnittstelle, auf die Sie über diesen Endpunkt zugreifen möchten.

Feld	Beschreibung
Nicht Vertrauenswürdiges Client-Netzwerk	Wählen Sie **Ja**, wenn dieser Endpunkt für nicht vertrauenswürdige Client-Netzwerke zugänglich sein soll. Andernfalls wählen Sie **Nein**. Wenn Sie **Yes** auswählen, ist der Port auf allen nicht vertrauenswürdigen Client-Netzwerken geöffnet. **Hinweis**: Sie können einen Port nur so konfigurieren, dass er für nicht vertrauenswürdige Client-Netzwerke geöffnet oder geschlossen wird, wenn Sie den Load Balancer-Endpunkt erstellen.

1. Wählen Sie **Weiter**.

Wählen Sie einen Bindungsmodus aus

Schritte

1. Wählen Sie einen Bindungsmodus für den Endpunkt aus, um den Zugriff auf den Endpunkt über eine beliebige IP-Adresse oder über spezifische IP-Adressen und Netzwerkschnittstellen zu steuern.

   Einige Bindungsmodi stehen entweder für Client-Endpunkte oder für Managementschnittstellen zur Verfügung. Hier sind alle Modi für beide Endpunkttypen aufgeführt.

Modus	Beschreibung
Global (Standard für Client-Endpunkte)	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 Einstellung **Global**, es sei denn, Sie müssen den Zugriff auf diesen Endpunkt einschränken.
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 (nur Client-Endpunkte)	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.

Modus	Beschreibung
Alle Admin-Nodes (Standard für Endpunkte der Managementoberfläche)	Clients müssen die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.

Wenn mehr als ein Endpunkt denselben Port verwendet, verwendet StorageGRID diese Prioritätsreihenfolge, um zu entscheiden, welcher Endpunkt verwendet werden soll: **Virtuelle IPs von HA-Gruppen** > **Knotenschnittstellen** > **Knotentyp** > **global**.

Wenn Sie Endpunkte der Managementoberfläche erstellen, sind nur Admin-Nodes zulässig.

2. Wenn Sie **virtuelle IPs von HA-Gruppen** ausgewählt haben, wählen Sie eine oder mehrere HA-Gruppen aus.

   Wenn Sie Endpunkte für die Managementoberfläche erstellen, wählen Sie VIPs aus, die nur Admin-Nodes zugeordnet sind.

3. Wenn Sie **Node-Schnittstellen** ausgewählt haben, wählen Sie für jeden Admin-Node oder Gateway-Node eine oder mehrere Node-Schnittstellen aus, die mit diesem Endpunkt verknüpft werden sollen.
4. Wenn Sie **Node type** ausgewählt haben, wählen Sie entweder Admin-Nodes aus, die sowohl den primären Admin-Node als auch alle nicht-primären Admin-Nodes enthalten, oder Gateway-Nodes.

Kontrolle des Mandantenzugriffs

> Ein Endpunkt der Managementoberfläche kann den Mandantenzugriff nur steuern, wenn der Endpunkt über den verfügt Schnittstellentyp des Tenant Manager.

Schritte

1. 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. Sie müssen diese Option auswählen, wenn Sie noch keine Mandantenkonten erstellt haben. Nachdem Sie Mandantenkonten hinzugefügt haben, können Sie den Load Balancer-Endpunkt bearbeiten, um bestimmte Konten zuzulassen oder zu blockieren.
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.

2. Wenn Sie einen **HTTP**-Endpunkt erstellen, müssen Sie kein Zertifikat anhängen. Wählen Sie **Erstellen**, um den neuen Load Balancer-Endpunkt hinzuzufügen. Fahren Sie dann mit fort Nachdem Sie fertig sind.

Andernfalls wählen Sie **Weiter**, um das Zertifikat anzuhängen.

Zertifikat anhängen

Schritte

1. Wenn Sie einen **HTTPS**-Endpunkt erstellen, wählen Sie den Typ des Sicherheitszertifikats aus, das Sie an den Endpunkt anhängen möchten.

   Das Zertifikat sichert die Verbindungen zwischen S3- und Swift-Clients und dem Load Balancer-Service auf Admin-Node oder Gateway-Nodes.

   - **Zertifikat hochladen**. Wählen Sie diese Option aus, wenn Sie über benutzerdefinierte Zertifikate zum Hochladen verfügen.
   - **Zertifikat generieren**. Wählen Sie diese Option aus, wenn Sie über die Werte verfügen, die zum Generieren eines benutzerdefinierten Zertifikats erforderlich sind.
   - **Verwenden Sie StorageGRID S3 und Swift Zertifikat**. Wählen Sie diese Option aus, wenn Sie das globale S3- und Swift-API-Zertifikat verwenden möchten, das auch für direkte Verbindungen zu Storage-Nodes verwendet werden kann.

     Sie können diese Option nur auswählen, wenn Sie das von der Grid-CA signierte Standard-API-Zertifikat S3 und Swift durch ein benutzerdefiniertes Zertifikat ersetzt haben, das von einer externen Zertifizierungsstelle signiert wurde. Siehe "Konfigurieren von S3- und Swift-API-Zertifikaten".

   - **Management Interface Zertifikat** verwenden. Wählen Sie diese Option aus, wenn Sie das Zertifikat für die globale Verwaltungsschnittstelle verwenden möchten, das auch für direkte Verbindungen zu Admin-Knoten verwendet werden kann.
2. Wenn Sie das StorageGRID S3- und Swift-Zertifikat nicht verwenden, laden Sie das Zertifikat hoch oder generieren Sie es.

Zertifikat hochladen

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatdateien hoch:

- **Server-Zertifikat**: Die benutzerdefinierte Server-Zertifikatdatei in PEM-Kodierung.
- **Zertifikat privater Schlüssel**: Die benutzerdefinierte Server Zertifikat private Schlüssel Datei (`.key`).

> Private EC-Schlüssel müssen 224 Bit oder größer sein. RSA Private Keys müssen mindestens 2048 Bit groß sein.

- **CA-Paket**: Eine einzelne optionale Datei, die die Zertifikate jeder Intermediate-Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.

c. Erweitern Sie **Zertifikatdetails**, um die Metadaten für jedes hochgeladene Zertifikat anzuzeigen. Wenn Sie ein optionales CA-Paket hochgeladen haben, wird jedes Zertifikat auf seiner eigenen Registerkarte angezeigt.

- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern, oder wählen Sie **CA-Paket herunterladen**, um das Zertifikatspaket zu speichern.

  Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

  Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat kopieren PEM** oder **CA-Paket kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.

d. Wählen Sie **Erstellen**.
Der Endpunkt des Load Balancer wird erstellt. Das benutzerdefinierte Zertifikat wird für alle nachfolgenden neuen Verbindungen zwischen S3- und Swift-Clients oder der Managementoberfläche und dem Endpunkt verwendet.

Zertifikat wird generiert

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domain-Name	Mindestens ein vollständig qualifizierter Domänenname, der in das Zertifikat aufgenommen werden soll. Verwenden Sie ein * als Platzhalter, um mehrere Domain-Namen darzustellen.
IP	Mindestens eine IP-Adresse, die in das Zertifikat aufgenommen werden soll.

Feld	Beschreibung
Betreff (optional)	X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers. Wenn in diesem Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domänennamen oder die IP-Adresse als allgemeinen Studienteilnehmer (CN).
Tage gültig	Anzahl der Tage nach Erstellung, nach denen das Zertifikat abläuft.
Fügen Sie wichtige Nutzungserweiterungen hinzu	Wenn diese Option ausgewählt ist (Standard und empfohlen), werden die Schlüsselnutzung und die erweiterten Schlüsselnutzungserweiterungen dem generierten Zertifikat hinzugefügt. Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist. **Hinweis**: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Erzeugen**.

d. Wählen Sie **Zertifikatdetails**, um die Metadaten für das generierte Zertifikat anzuzeigen.

   - Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern.

     Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.

e. Wählen Sie **Erstellen**.

   Der Endpunkt des Load Balancer wird erstellt. Das benutzerdefinierte Zertifikat wird für alle nachfolgenden neuen Verbindungen zwischen S3- und Swift-Clients oder der Managementoberfläche und diesem Endpunkt verwendet.

Nachdem Sie fertig sind

Schritte

1. Wenn Sie einen DNS verwenden, stellen Sie sicher, dass der DNS einen Datensatz enthält, mit dem der vollständig qualifizierte StorageGRID-Domänenname (FQDN) jeder IP-Adresse zugeordnet wird, die Clients zum Verbindungsaufbau verwenden.

   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, stellen Clients eine Verbindung zu den virtuellen IP-Adressen dieser HA-Gruppe her.
- Wenn Sie keine HA-Gruppe verwenden, stellen Clients mithilfe der IP-Adresse eines Gateway-Node oder Admin-Node eine Verbindung zum StorageGRID Load Balancer-Service her.

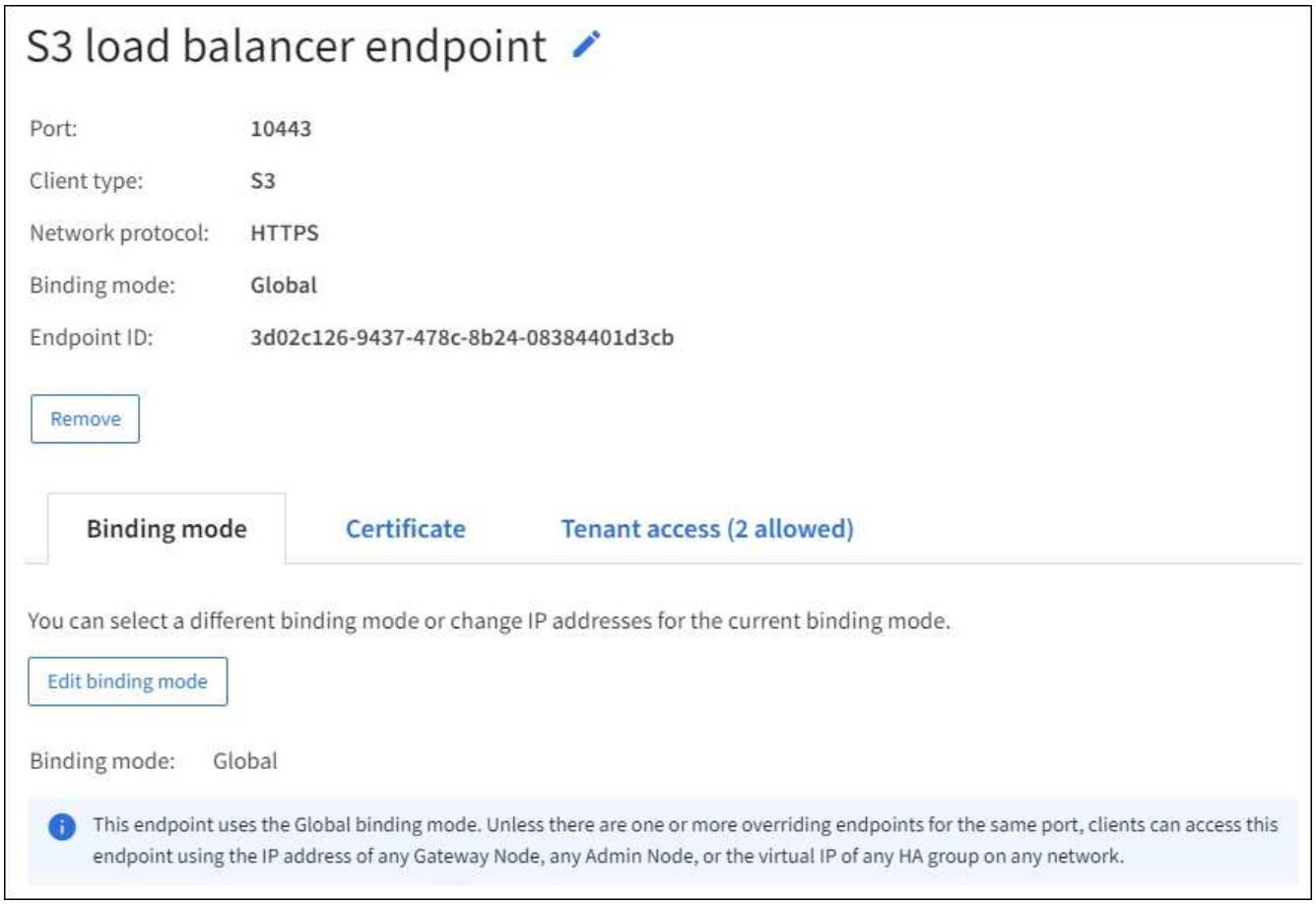
  Außerdem müssen Sie sicherstellen, dass der DNS-Datensatz alle erforderlichen Endpunkt-Domain-Namen referenziert, einschließlich Platzhalternamen.

2. S3- und Swift-Clients erhalten die für die Verbindung mit dem Endpunkt erforderlichen Informationen:
   - Port-Nummer
   - Vollständig qualifizierter Domain-Name oder IP-Adresse
   - Alle erforderlichen Zertifikatsdetails

Load Balancer-Endpunkte anzeigen und bearbeiten

Sie können Details zu vorhandenen Load Balancer-Endpunkten anzeigen, einschließlich der Zertifikatmetadaten für einen gesicherten Endpunkt. Sie können bestimmte Einstellungen für einen Endpunkt ändern.

- Um grundlegende Informationen für alle Lastausgleichsendpunkte anzuzeigen, lesen Sie die Tabellen auf der Seite Lastausgleichsendpunkte.
- Um alle Details zu einem bestimmten Endpunkt einschließlich Zertifikatmetadaten anzuzeigen, wählen Sie in der Tabelle den Namen des Endpunkts aus. Die angezeigten Informationen variieren je nach Endpunkttyp und Konfiguration.



- Um einen Endpunkt zu bearbeiten, verwenden Sie das Menü **actions** auf der Seite Load Balancer Endpoints.

> Wenn Sie den Zugriff auf Grid Manager während der Bearbeitung des Ports eines Endpunkts der Managementoberfläche verlieren, aktualisieren Sie die URL und den Port, um den Zugriff wiederherzustellen.

> Nach dem Bearbeiten eines Endpunkts müssen Sie möglicherweise bis zu 15 Minuten warten, bis Ihre Änderungen auf alle Nodes angewendet werden.

Aufgabe	Menü „Aktionen“	Detailseite
Endpunktname bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** > **Endpunktname bearbeiten** aus. c. Geben Sie den neuen Namen ein. d. Wählen Sie **Speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie das Bearbeitungssymbol . c. Geben Sie den neuen Namen ein. d. Wählen Sie **Speichern**.
Endpunkt-Port bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **actions** > **Edit Endpoint Port** c. Geben Sie eine gültige Portnummer ein. d. Wählen Sie **Speichern**.	*N/a*
Endpunktbindungsmodus bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** > **Endpunktbindungsmodus bearbeiten**. c. Aktualisieren Sie den Bindungsmodus, falls erforderlich. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie **Bindungsmodus bearbeiten**. c. Aktualisieren Sie den Bindungsmodus, falls erforderlich. d. Wählen Sie **Änderungen speichern**.

Aufgabe	Menü „Aktionen“	Detailseite
Endpunktzertifikat bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** > **Endpunktzertifikat bearbeiten** aus. c. Laden Sie ein neues benutzerdefiniertes Zertifikat hoch oder erstellen Sie es, falls erforderlich, mit der Verwendung des globalen S3- und Swift-Zertifikats. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte **Zertifikat** aus. c. Wählen Sie **Zertifikat bearbeiten**. d. Laden Sie ein neues benutzerdefiniertes Zertifikat hoch oder erstellen Sie es, falls erforderlich, mit der Verwendung des globalen S3- und Swift-Zertifikats. e. Wählen Sie **Änderungen speichern**.
Bearbeiten Sie den Mandantenzugriff	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **actions** > **Edit Tenant Access**. c. Wählen Sie eine andere Zugriffsoption aus, wählen Sie Mandanten aus der Liste aus oder entfernen Sie sie aus oder führen Sie beides aus. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte **Tenant Access**. c. Wählen Sie **Mandantenzugriff bearbeiten**. d. Wählen Sie eine andere Zugriffsoption aus, wählen Sie Mandanten aus der Liste aus oder entfernen Sie sie aus oder führen Sie beides aus. e. Wählen Sie **Änderungen speichern**.

Entfernen Sie Load Balancer-Endpunkte

Sie können einen oder mehrere Endpunkte über das Menü **Aktionen** entfernen oder einen einzelnen Endpunkt von der Detailseite entfernen.

> Um Client-Unterbrechungen zu vermeiden, aktualisieren Sie die betroffenen S3- oder Swift-Client-Applikationen, bevor Sie einen Load Balancer-Endpunkt entfernen. Aktualisieren Sie jeden Client, um eine Verbindung über einen Port herzustellen, der einem anderen Load Balancer-Endpunkt zugewiesen ist. Aktualisieren Sie auch die erforderlichen Zertifikatsinformationen.

> Wenn Sie den Zugriff auf Grid Manager verlieren, während Sie einen Endpunkt der Managementoberfläche entfernen, aktualisieren Sie die URL.

- So entfernen Sie einen oder mehrere Endpunkte:
  a. Aktivieren Sie auf der Seite Load Balancer das Kontrollkästchen für jeden Endpunkt, den Sie entfernen möchten.
  b. Wählen Sie **Aktionen** > **Entfernen**.
  c. Wählen Sie **OK**.

- So entfernen Sie einen Endpunkt auf der Detailseite:
  a. Auf der Seite Load Balancer. Wählen Sie den Endpunktnamen aus.
  b. Wählen Sie auf der Detailseite * Entfernen.
  c. Wählen Sie **OK**.