



Konfigurieren von S3- und Swift-Client-Verbindungen

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

- Konfigurieren von S3- und Swift-Client-Verbindungen 1
 - Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen 1
 - Managen des Lastausgleichs 4
 - Verwalten von nicht vertrauenswürdigen Client-Netzwerken 14
 - Verwalten von Hochverfügbarkeitsgruppen 16
- Konfigurieren von S3-API-Endpunkt-Domain-Namen 29
- Aktivieren von HTTP für die Clientkommunikation 31
- Steuern, welche Client-Operationen zulässig sind 32

Konfigurieren von S3- und Swift-Client-Verbindungen

Als Grid-Administrator managen Sie die Konfigurationsoptionen, die steuern, wie S3- und Swift-Mandanten Client-Applikationen mit Ihrem StorageGRID-System verbinden können, um Daten zu speichern und abzurufen. Es stehen verschiedene Optionen zur Verfügung, um verschiedene Anforderungen von Kunden und Mandanten zu erfüllen.

Client-Applikationen können Objekte speichern oder abrufen, indem sie eine Verbindung mit folgenden Komponenten herstellen:

- Der Lastverteilungsservice an Admin-Nodes oder Gateway-Nodes oder optional die virtuelle IP-Adresse einer HA-Gruppe (High Availability, Hochverfügbarkeit) von Admin-Nodes oder Gateway-Nodes
- Der CLB-Dienst auf Gateway-Knoten oder optional die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe von Gateway-Knoten



Der CLB-Service ist veraltet. Clients, die vor der Version StorageGRID 11.3 konfiguriert wurden, können den CLB-Service auf Gateway-Knoten weiterhin verwenden. Alle anderen Client-Applikationen, die zum Lastausgleich vom StorageGRID abhängig sind, sollten über den Load Balancer Service eine Verbindung herstellen.

- Storage-Nodes mit oder ohne externen Load Balancer

Auf dem StorageGRID-System können Sie optional die folgenden Funktionen konfigurieren:

- **Load Balancer Service:** Sie ermöglichen Clients die Verwendung des Load Balancer Service durch die Erstellung von Load Balancer Endpunkten für Client-Verbindungen. Beim Erstellen eines Load Balancer-Endpunkts geben Sie eine Portnummer an, ob der Endpunkt HTTP- oder HTTPS-Verbindungen akzeptiert, der Client-Typ (S3 oder Swift), der den Endpunkt verwendet, und das Zertifikat, das für HTTPS-Verbindungen verwendet werden soll (falls zutreffend).
- **UnTrusted Client Network:** Sie können das Client-Netzwerk sicherer machen, indem Sie es als unvertrauenswürdig konfigurieren. Wenn das Client-Netzwerk nicht vertrauenswürdig ist, können Clients nur über Load Balancer-Endpunkte eine Verbindung herstellen.
- **Hochverfügbarkeitsgruppen:** Sie können eine HA-Gruppe von Gateway-Knoten oder Admin-Nodes erstellen, um eine aktiv-Backup-Konfiguration zu erstellen, oder Round-Robin-DNS oder einen Load Balancer eines Drittanbieters und mehrere HA-Gruppen verwenden, um eine aktiv/aktiv-Konfiguration zu erreichen. Client-Verbindungen werden mithilfe der virtuellen IP-Adressen der HA-Gruppen hergestellt.

Sie können auch die Verwendung von HTTP für Clients aktivieren, die eine Verbindung zu StorageGRID entweder direkt zu Storage-Nodes oder über den CLB-Dienst (veraltet) herstellen, und Sie können S3-API-Endpunktdomännennamen für S3-Clients konfigurieren.

Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen

Client-Applikationen können sich mithilfe der IP-Adresse eines Grid-Node und der Port-Nummer eines Service auf diesem Node mit StorageGRID verbinden. Bei Konfiguration von Hochverfügbarkeitsgruppen (High Availability, HA) können Client-Applikationen eine

Verbindung über die virtuelle IP-Adresse der HA-Gruppe herstellen.

Über diese Aufgabe

In dieser Tabelle sind die verschiedenen Verbindungsmethoden aufgeführt, mit denen Clients eine Verbindung zu StorageGRID herstellen können, sowie die für den jeweiligen Verbindungstyp verwendeten IP-Adressen und Ports. Die Anleitung beschreibt das Auffinden dieser Informationen im Grid Manager, wenn die Endpunkte des Load Balancer und Gruppen für Hochverfügbarkeit (HA) bereits konfiguriert sind.

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
HA-Gruppe	Lastausgleich	Virtuelle IP-Adresse einer HA-Gruppe	<ul style="list-style-type: none"> • Endpunkt-Port des Load Balancer
HA-Gruppe	CLB Hinweis: der CLB-Service ist veraltet.	Virtuelle IP-Adresse einer HA-Gruppe	S3-Standard-Ports: <ul style="list-style-type: none"> • HTTPS: 8082 • HTTP: 8084 Swift-Standardports: <ul style="list-style-type: none"> • HTTPS:8083 • HTTP:8085
Admin-Node	Lastausgleich	IP-Adresse des Admin-Knotens	<ul style="list-style-type: none"> • Endpunkt-Port des Load Balancer
Gateway-Node	Lastausgleich	IP-Adresse des Gateway-Node	<ul style="list-style-type: none"> • Endpunkt-Port des Load Balancer
Gateway-Node	CLB Hinweis: der CLB-Service ist veraltet.	IP-Adresse des Gateway-Node Hinweis: standardmäßig sind HTTP-Ports für CLB und LDR nicht aktiviert.	S3-Standard-Ports: <ul style="list-style-type: none"> • HTTPS: 8082 • HTTP: 8084 Swift-Standardports: <ul style="list-style-type: none"> • HTTPS:8083 • HTTP:8085
Storage-Node	LDR	IP-Adresse des Speicherknoten	S3-Standard-Ports: <ul style="list-style-type: none"> • HTTPS: 18082 • HTTP: 18084 Swift-Standardports: <ul style="list-style-type: none"> • HTTPS: 18083 • HTTP:18085

Beispiele

Verwenden Sie eine strukturierte URL, wie unten gezeigt, um einen S3-Client mit dem Load Balancer-Endpunkt einer HA-Gruppe von Gateway-Nodes zu verbinden:

- `https://VIP-of-HA-group:LB-endpoint-port`

Wenn beispielsweise die virtuelle IP-Adresse der HA-Gruppe 192.0.2.5 lautet und die Portnummer eines S3 Load Balancer Endpunkts 10443 ist, kann ein S3-Client die folgende URL zur Verbindung mit StorageGRID verwenden:

- `https://192.0.2.5:10443`

Verwenden Sie eine strukturierte URL, wie unten gezeigt, um einen Swift-Client mit dem Load Balancer-Endpunkt einer HA-Gruppe von Gateway-Nodes zu verbinden:

- `https://VIP-of-HA-group:LB-endpoint-port`

Wenn beispielsweise die virtuelle IP-Adresse der HA-Gruppe 192.0.2.6 lautet und die Portnummer eines Swift Load Balancer Endpunkts 10444 ist, kann ein Swift-Client die folgende URL zur Verbindung mit StorageGRID verwenden:

- `https://192.0.2.6:10444`

Ein DNS-Name kann für die IP-Adresse konfiguriert werden, die Clients zum Herstellen der Verbindung mit StorageGRID verwenden. Wenden Sie sich an Ihren Netzwerkadministrator vor Ort.

Schritte

1. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.
2. So suchen Sie die IP-Adresse eines Grid-Knotens:
 - a. Wählen Sie **Knoten**.
 - b. Wählen Sie den Admin-Node, Gateway-Node oder Storage-Node aus, mit dem Sie eine Verbindung herstellen möchten.
 - c. Wählen Sie die Registerkarte **Übersicht**.
 - d. Notieren Sie im Abschnitt Node-Informationen die IP-Adressen für den Node.
 - e. Klicken Sie auf **Mehr anzeigen**, um IPv6-Adressen und Schnittstellen-Zuordnungen anzuzeigen.

Sie können Verbindungen von Client-Anwendungen zu einer beliebigen IP-Adresse in der Liste herstellen:

- **Eth0:** Grid Network
- **Eth1:** Admin-Netzwerk (optional)
- **Eth2:** Client-Netzwerk (optional)



Wenn ein Admin-Node oder ein Gateway-Node angezeigt wird und dieser in einer Hochverfügbarkeitsgruppe der aktive Node ist, wird auf eth2 die virtuelle IP-Adresse der HA-Gruppe angezeigt.

3. So finden Sie die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe:
 - a. Wählen Sie **Konfiguration > Netzwerkeinstellungen > Hochverfügbarkeitsgruppen**.

- b. Notieren Sie in der Tabelle die virtuelle IP-Adresse der HA-Gruppe.
4. So finden Sie die Portnummer eines Load Balancer-Endpunkts:
 - a. Wählen Sie **Konfiguration > Netzwerkeinstellungen > Balancer-Endpunkte Laden**.

Die Seite Load Balancer Endpoints wird angezeigt und zeigt die Liste der bereits konfigurierten Endpunkte an.
 - b. Wählen Sie einen Endpunkt aus, und klicken Sie auf **Endpunkt bearbeiten**.

Das Fenster Endpunkt bearbeiten wird geöffnet und zeigt weitere Details zum Endpunkt an.
 - c. Bestätigen Sie, dass der ausgewählte Endpunkt für die Verwendung mit dem korrekten Protokoll konfiguriert ist (S3 oder Swift), und klicken Sie dann auf **Abbrechen**.
 - d. Notieren Sie sich die Portnummer für den Endpunkt, den Sie für eine Clientverbindung verwenden möchten.



Wenn die Portnummer 80 oder 443 ist, wird der Endpunkt nur auf Gateway-Knoten konfiguriert, da diese Ports auf Admin-Nodes reserviert sind. Alle anderen Ports werden sowohl an Gateway-Knoten als auch an Admin-Nodes konfiguriert.

Managen des Lastausgleichs

Die StorageGRID Lastausgleichsfunktionen verarbeiten Aufnahme- und Abruf-Workloads von S3 und Swift Clients. Durch Verteilung der Workloads und Verbindungen auf mehrere Storage-Nodes maximiert der Lastausgleich die Geschwindigkeit und die Kapazität der Verbindungen.

Es gibt folgende Möglichkeiten für den Lastausgleich in Ihrem StorageGRID System:

- Verwenden Sie den Lastverteilungsservice, der auf Admin Nodes und Gateway Nodes installiert ist. Der Lastverteilungsservice bietet Layer 7 Load Balancing und führt TLS-Terminierung von Client-Anfragen durch, prüft die Anfragen und stellt neue sichere Verbindungen zu den Storage Nodes her. Dies ist der empfohlene Lastausgleichmechanismus.
- Verwenden Sie den Service Connection Load Balancer (CLB), der nur auf Gateway Nodes installiert ist. Der CLB-Service bietet Layer 4-Lastenausgleich und unterstützt Verbindungskosten.



Der CLB-Service ist veraltet.

- Integration eines Load Balancer eines Drittanbieters: Genaue Informationen erhalten Sie bei Ihrem NetApp Ansprechpartner.

Wie funktioniert der Lastausgleich? Load Balancer Service

Der Load Balancer Service verteilt eingehende Netzwerkverbindungen von Client-Anwendungen auf Storage Nodes. Um den Lastenausgleich zu aktivieren, müssen Sie Load Balancer-Endpunkte mithilfe des Grid-Managers konfigurieren.

Sie können Load Balancer-Endpunkte nur für Admin-Nodes oder Gateway-Nodes konfigurieren, da diese Node-Typen den Load Balancer Service enthalten. Sie können keine Endpunkte für Speicherknoten oder

Knoten archivieren konfigurieren.

Jeder Load Balancer-Endpunkt legt einen Port, ein Protokoll (HTTP oder HTTPS), einen Servicetyp (S3 oder Swift) und einen Bindungsmodus fest. HTTPS-Endpunkte erfordern ein Serverzertifikat. Bindungsmodi ermöglichen es Ihnen, die Zugriffsmöglichkeiten von Endpunktports auf folgende Arten zu beschränken:

- Spezifische virtuelle Hochverfügbarkeits-IP-Adressen (VIPs)
- Spezielle Netzwerkschnittstellen bestimmter Nodes

Überlegungen zu Ports

Clients können auf alle Endpunkte zugreifen, die Sie auf jedem Node konfigurieren, auf dem der Load Balancer Service ausgeführt wird. Es gibt zwei Ausnahmen: Die Ports 80 und 443 sind auf Admin-Nodes reserviert, sodass auf diesen Ports konfigurierte Endpunkte nur auf Gateway-Knoten Lastverteilungsvorgänge unterstützen.

Wenn Sie Ports neu zugeordnet haben, können Sie nicht dieselben Ports zum Konfigurieren von Load Balancer-Endpunkten verwenden. Sie können Endpunkte mit neu zugeordneten Ports erstellen, aber diese Endpunkte werden nicht dem Load Balancer-Service, sondern den ursprünglichen CLB-Ports und -Service neu zugeordnet. Befolgen Sie die Schritte in der Recovery- und Wartungsanleitung zum Entfernen von Port-Remaps.



Der CLB-Service ist veraltet.

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.

Verwandte Informationen

["Verwalten Sie erholen"](#)

Konfigurieren von Load Balancer-Endpunkten

Sie können Load Balancer-Endpunkte erstellen, bearbeiten und entfernen.

Erstellen von Load Balancer-Endpunkten

Jeder Load Balancer-Endpunkt legt einen Port, ein Netzwerkprotokoll (HTTP oder HTTPS) und einen Servicetyp (S3 oder Swift) fest. Wenn Sie einen HTTPS-Endpunkt erstellen, müssen Sie ein Serverzertifikat hochladen oder erstellen.

Was Sie benötigen

- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Wenn Sie zuvor Ports neu zugeordnet haben, die Sie für den Load Balancer-Dienst verwenden möchten, müssen Sie die Neuzuordnungen entfernt haben.



Wenn Sie Ports neu zugeordnet haben, können Sie nicht dieselben Ports zum Konfigurieren von Load Balancer-Endpunkten verwenden. Sie können Endpunkte mit neu zugeordneten Ports erstellen, aber diese Endpunkte werden nicht dem Load Balancer-Service, sondern den ursprünglichen CLB-Ports und -Service neu zugeordnet. Befolgen Sie die Schritte in der Recovery- und Wartungsanleitung zum Entfernen von Port-Remaps.



Der CLB-Service ist veraltet.

Schritte

1. Wählen Sie **Konfiguration > Netzwerkeinstellungen > Balancer-Endpunkte Laden**.

Die Seite Load Balancer Endpoints wird angezeigt.

Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

Changes to endpoints can take up to 15 minutes to be applied to all nodes.

[+ Add endpoint port](#) [Edit endpoint](#) [Remove endpoint port](#)

Display name	Port	Using HTTPS
<i>No endpoints configured.</i>		

2. Wählen Sie **Endpunkt hinzufügen**.

Das Dialogfeld Endpunkt erstellen wird angezeigt.

Create Endpoint

Display Name

Port

10443

Protocol

HTTP

HTTPS

Endpoint Binding Mode

Global

HA Group VIPs

Node Interfaces

Cancel

Save

3. Geben Sie einen Anzeigenamen für den Endpunkt ein, der in der Liste auf der Seite Load Balancer Endpoints angezeigt wird.
4. Geben Sie eine Portnummer ein, oder lassen Sie die vorausgefüllte Portnummer unverändert.

Wenn Sie die Portnummer 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Knoten konfiguriert, da diese Ports auf Admin-Nodes reserviert sind.



Von anderen Grid-Services verwendete Ports sind nicht zulässig. In den Netzwerkrichtlinien finden Sie eine Liste der Ports, die für die interne und externe Kommunikation verwendet werden.

5. Wählen Sie **HTTP** oder **HTTPS** aus, um das Netzwerkprotokoll für diesen Endpunkt festzulegen.

6. Wählen Sie einen Endpunktbindungsmodus aus.

- **Global** (Standard): Der Endpunkt ist auf allen Gateway Nodes und Admin Nodes auf der angegebenen Portnummer zugänglich.

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

This endpoint is currently bound globally. All nodes will use this endpoint unless an endpoint with an overriding binding mode exists for a specific port.

- **HA Group VIPs**: Der Endpunkt ist nur über die für die ausgewählten HA-Gruppen definierten virtuellen IP-Adressen zugänglich. In diesem Modus definierte Endpunkte können die gleiche Port-Nummer wiederverwenden, solange die von diesen Endpunkten definierten HA-Gruppen nicht miteinander überlappen.

Wählen Sie die HA-Gruppen mit den virtuellen IP-Adressen aus, auf denen der Endpunkt angezeigt werden soll.

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

Name	Description	Virtual IP Addresses	Interfaces
<input type="checkbox"/> Group1		192.168.5.163	CO-REF-DC1-ADM1:eth0 (preferred Master)
<input type="checkbox"/> Group2		47.47.5.162	CO-REF-DC1-ADM1:eth2 (preferred Master)

Displaying 2 HA groups.

No HA groups selected. You must select one or more HA Groups; otherwise, this endpoint will act as a globally bound endpoint.

- **Node-Schnittstellen**: Der Endpunkt ist nur auf den angegebenen Knoten und den Netzwerkschnittstellen zugänglich. In diesem Modus definierte Endpunkte können dieselbe

Portnummer wiederverwenden, solange sich diese Schnittstellen nicht gegenseitig überschneiden.

Wählen Sie die Knotenschnittstellen aus, auf denen der Endpunkt angezeigt werden soll.

Create Endpoint


Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

Node	Interface
<input type="checkbox"/> CO-REF-DC1-ADM1	eth0
<input type="checkbox"/> CO-REF-DC1-ADM1	eth1
<input type="checkbox"/> CO-REF-DC1-ADM1	eth2
<input type="checkbox"/> CO-REF-DC1-GW1	eth0
<input type="checkbox"/> CO-REF-DC2-ADM1	eth0
<input type="checkbox"/> CO-REF-DC2-GW1	eth0

 No node interfaces selected. You must select one or more node interfaces; otherwise, this endpoint will act as a globally bound endpoint.

7. Wählen Sie **Speichern**.

Das Dialogfeld Endpunkt bearbeiten wird angezeigt.

8. Wählen Sie **S3** oder **Swift** aus, um den Verkehrstyp festzulegen, den dieser Endpunkt bedienen wird.

Edit Endpoint Unsecured Port A (port 10449)

Endpoint Service Configuration

Endpoint service type S3 Swift

9. Wenn Sie **HTTP** ausgewählt haben, wählen Sie **Speichern**.

Der ungesicherte Endpunkt wird erstellt. In der Tabelle auf der Seite Load Balancer Endpoints werden der Anzeigename, die Portnummer, das Protokoll und die Endpunkt-ID des Endpunkts aufgeführt.

10. Wenn Sie **HTTPS** ausgewählt haben und ein Zertifikat hochladen möchten, wählen Sie **Zertifikat hochladen**.

Load Certificate

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

Server Certificate

Certificate Private Key

CA Bundle

Cancel

Save

- a. Suchen Sie nach dem Serverzertifikat und dem privaten Zertifikatschlüssel.

Damit S3-Clients eine Verbindung über einen S3-API-Endpoint-Domain-Namen herstellen können, verwenden Sie ein Multi-Domain- oder Platzhalterzertifikat, das mit allen Domännennamen übereinstimmt, die der Client zum Herstellen der Verbindung zum Grid verwenden kann. Beispielsweise kann das Serverzertifikat den Domännennamen verwenden `*.example.com`.

"Konfigurieren von S3-API-Endpoint-Domain-Namen"

- a. Optional können Sie nach einem CA-Bundle suchen.
- b. Wählen Sie **Speichern**.

Die PEM-kodierten Zertifikatdaten für den Endpunkt werden angezeigt.

11. Wenn Sie **HTTPS** ausgewählt haben und ein Zertifikat erstellen möchten, wählen Sie **Zertifikat erstellen**.

Generate Certificate

Domain 1

IP 1

Subject

Days valid

Cancel

Generate

- a. Geben Sie einen Domain-Namen oder eine IP-Adresse ein.

Sie können Platzhalter verwenden, um die vollständig qualifizierten Domännennamen aller Admin-Nodes und Gateway-Nodes darzustellen, auf denen der Load Balancer Service ausgeführt wird. Beispiel: `*.sgws.foo.com` Verwendet den Platzhalter `*` für die Darstellung `gn1.sgws.foo.com` Und

gn2.sgws.foo.com.

"Konfigurieren von S3-API-Endpoint-Domain-Namen"

- a. Wählen Sie **+** So fügen Sie weitere Domain-Namen oder IP-Adressen hinzu:

Wenn Sie Hochverfügbarkeitsgruppen (HA-Gruppen) verwenden, fügen Sie die Domain-Namen und IP-Adressen der virtuellen HA-IPs hinzu.

- b. Geben Sie optional einen X.509-Studienteilnehmer ein, der auch als Distinguished Name (DN) bezeichnet wird, um zu ermitteln, wer das Zertifikat besitzt.
- c. Wählen Sie optional die Anzahl der Tage aus, an denen das Zertifikat gültig ist. Der Standardwert ist 730 Tage.
- d. Wählen Sie **Erzeugen**.

Die Zertifikatmetadaten und die PEM-kodierten Zertifikatdaten für den Endpoint werden angezeigt.

12. Klicken Sie Auf **Speichern**.

Der Endpoint wird erstellt. In der Tabelle auf der Seite Load Balancer Endpoints werden der Anzeigename, die Portnummer, das Protokoll und die Endpoint-ID des Endpunkts aufgeführt.

Verwandte Informationen

["Verwalten Sie erhalten"](#)

["Netzwerkrichtlinien"](#)

["Verwalten von Hochverfügbarkeitsgruppen"](#)

["Verwalten von nicht vertrauenswürdigen Client-Netzwerken"](#)

Bearbeiten von Load Balancer-Endpunkten

Für einen ungesicherten (HTTP) Endpoint können Sie den Dienstyp des Endpunkts zwischen S3 und Swift ändern. Für einen gesicherten Endpoint (HTTPS) können Sie den Dienstyp des Endpunkts bearbeiten und das Sicherheitszertifikat anzeigen oder ändern.

Was Sie benötigen

- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

1. Wählen Sie **Konfiguration > Netzwerkeinstellungen > Balancer-Endpunkte Laden**.

Die Seite Load Balancer Endpoints wird angezeigt. Die vorhandenen Endpunkte sind in der Tabelle aufgeführt.

Endpunkte mit bald auslaufenden Zertifikaten sind in der Tabelle aufgeführt.

- Ändern Sie den Endpunktbindungsmodus. Für einen gesicherten Endpunkt (HTTPS) können Sie:
- Ändern Sie den Endpunkt-Servicetyp zwischen S3 und Swift.
- Ändern Sie den Endpunktbindungsmodus.
- Zeigen Sie das Sicherheitszertifikat an.
- Hochladen oder Generieren eines neuen Sicherheitszertifikats, wenn das aktuelle Zertifikat abgelaufen ist oder kurz vor Ablauf steht.

Wählen Sie eine Registerkarte aus, um detaillierte Informationen zum StorageGRID-Standardserverzertifikat oder zum hochgeladenen Zertifikat einer Zertifizierungsstelle anzuzeigen.



Um das Protokoll für einen vorhandenen Endpunkt, zum Beispiel von HTTP zu HTTPS, zu ändern, müssen Sie einen neuen Endpunkt erstellen. Befolgen Sie die Anweisungen zum Erstellen von Load Balancer-Endpunkten, und wählen Sie das gewünschte Protokoll aus.

5. Klicken Sie Auf **Speichern**.

Verwandte Informationen

[Erstellen von Load Balancer-Endpunkten](#)

Entfernen von Load Balancer-Endpunkten

Wenn Sie keinen Endpunkt mehr für den Load Balancer benötigen, können Sie ihn entfernen.

Was Sie benötigen

- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Schritte

1. Wählen Sie **Konfiguration > Netzwerkeinstellungen > Balancer-Endpunkte Laden**.

Die Seite Load Balancer Endpoints wird angezeigt. Die vorhandenen Endpunkte sind in der Tabelle aufgeführt.

Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

<input type="button" value="+ Add endpoint"/> <input type="button" value="✎ Edit endpoint"/> <input type="button" value="✕ Remove endpoint"/>			
	Display name	Port	Using HTTPS
<input type="radio"/>	Unsecured Endpoint 5	10444	No
<input checked="" type="radio"/>	Secured Endpoint 1	10443	Yes

Displaying 2 endpoints.

2. Wählen Sie das Optionsfeld links neben dem Endpunkt, den Sie entfernen möchten.
3. Klicken Sie auf **Endpunkt entfernen**.

Ein Bestätigungsdialogfeld wird angezeigt.

Warning

Remove Endpoint

Are you sure you want to remove endpoint 'Secured Endpoint 1'?

Cancel

OK

4. Klicken Sie auf **OK**.

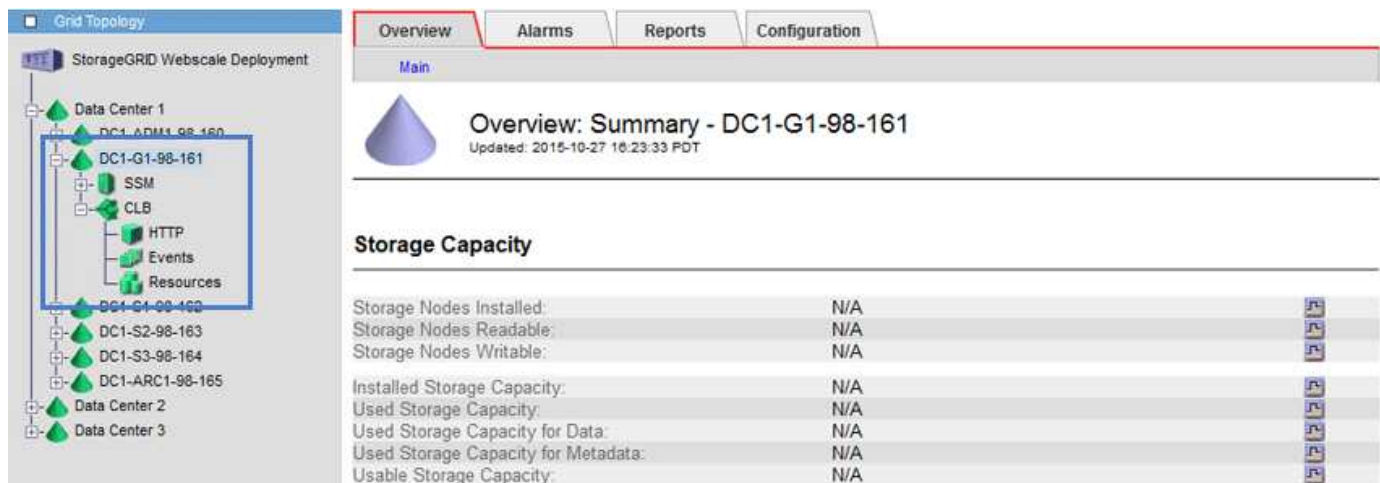
Der Endpunkt wird entfernt.

Wie der Lastenausgleich funktioniert - CLB-Service

Der CLB-Dienst (Connection Load Balancer) auf Gateway-Nodes ist veraltet. Der Lastausgleichsdienst ist jetzt der empfohlene Lastausgleichmechanismus.

Der CLB-Service nutzt Layer 4 Load Balancing zur Verteilung eingehender TCP-Netzwerkverbindungen von Client-Anwendungen auf den optimalen Storage Node basierend auf Verfügbarkeit, Systemlast und den vom Administrator konfigurierten Verbindungskosten. Wenn der optimale Speicherknoten ausgewählt wird, baut der CLB-Dienst eine zweiseitige Netzwerkverbindung auf und leitet den Datenverkehr vom und zum ausgewählten Knoten weiter. Beim CLB wird die Konfiguration des Grid-Netzwerks nicht berücksichtigt, wenn eingehende Netzwerkverbindungen geleitet werden.

Um Informationen zum CLB-Dienst anzuzeigen, wählen Sie **Support > Tools > Grid Topology** und erweitern Sie dann einen Gateway-Knoten, bis Sie **CLB** und die darunter stehenden Optionen auswählen können.



The screenshot shows the StorageGRID Webconsole interface. On the left, the 'Grid Topology' tree is expanded to show 'Data Center 1' > 'DC1-G1-98-161' > 'CLB'. On the right, the 'Overview: Summary - DC1-G1-98-161' page is displayed, updated on 2015-10-27 16:23:33 PDT. Below the title, there is a 'Storage Capacity' section with a table of metrics.

Storage Capacity	
Storage Nodes Installed:	N/A
Storage Nodes Readable:	N/A
Storage Nodes Writable:	N/A
Installed Storage Capacity:	N/A
Used Storage Capacity:	N/A
Used Storage Capacity for Data:	N/A
Used Storage Capacity for Metadata:	N/A
Usable Storage Capacity:	N/A

Wenn Sie den CLB-Service nutzen möchten, sollten Sie die Verbindungskosten für Ihr StorageGRID-System in Betracht ziehen.

Verwandte Informationen

["Was sind Verbindungskosten"](#)

["Verbindungskosten werden aktualisiert"](#)

Verwalten von nicht vertrauenswürdigen Client-Netzwerken

Wenn Sie ein Client-Netzwerk verwenden, können Sie StorageGRID vor feindlichen Angriffen schützen, indem Sie eingehenden Client-Datenverkehr nur auf explizit konfigurierten Endpunkten akzeptieren.

Standardmäßig ist das Client-Netzwerk auf jedem Grid-Knoten *Trusted*. Das heißt, StorageGRID vertraut standardmäßig eingehende Verbindungen zu jedem Grid-Knoten auf allen verfügbaren externen Ports (siehe Informationen über externe Kommunikation in den Netzwerkrichtlinien).

Sie können die Bedrohung durch feindliche Angriffe auf Ihrem StorageGRID-System verringern, indem Sie angeben, dass das Client-Netzwerk auf jedem Knoten *unvertrauenswürdig* ist. Wenn das Client-Netzwerk eines Node nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehende Verbindungen an Ports, die explizit als Load Balancer-Endpunkte konfiguriert sind.

Beispiel 1: Der Gateway-Node akzeptiert nur HTTPS-S3-Anforderungen

Angenommen, ein Gateway-Node soll den gesamten eingehenden Datenverkehr im Client-Netzwerk mit Ausnahme von HTTPS S3-Anforderungen ablehnen. Sie würden folgende allgemeine Schritte durchführen:

1. Konfigurieren Sie auf der Seite Load Balancer Endpoints einen Endpunkt für den Load Balancer für S3 über HTTPS am Port 443.
2. Geben Sie auf der Seite nicht vertrauenswürdige Clientnetzwerke an, dass das Client-Netzwerk auf dem Gateway-Node nicht vertrauenswürdig ist.

Nachdem Sie Ihre Konfiguration gespeichert haben, wird der gesamte eingehende Datenverkehr im Client-Netzwerk des Gateway-Knotens außer HTTPS-S3-Anfragen auf Port 443- und ICMP-Echo-(Ping-)Anfragen verworfen.

Beispiel 2: Storage-Node sendet Anforderungen von S3-Plattform-Services

Angenommen, Sie möchten den Datenverkehr des Outbound-S3-Platfordienstes von einem Speicherknoten aktivieren, jedoch eingehende Verbindungen zu diesem Storage-Node im Client-Netzwerk verhindern. Sie würden diesen allgemeinen Schritt durchführen:

- Geben Sie auf der Seite nicht vertrauenswürdige Clientnetzwerke an, dass das Client-Netzwerk auf dem Speicherknoten nicht vertrauenswürdig ist.

Nachdem Sie Ihre Konfiguration gespeichert haben, akzeptiert der Speicherknoten keinen eingehenden Datenverkehr im Client-Netzwerk mehr, aber er erlaubt weiterhin ausgehende Anfragen an Amazon Web Services.

Verwandte Informationen

["Netzwerkrichtlinien"](#)

["Konfigurieren von Load Balancer-Endpunkten"](#)

Das Festlegen des Client-Netzwerks eines Knotens ist nicht vertrauenswürdig

Wenn Sie ein Client-Netzwerk verwenden, können Sie angeben, ob das Client-Netzwerk jedes Node vertrauenswürdig oder nicht vertrauenswürdig ist. Sie können auch die Standardeinstellung für neue Knoten festlegen, die in einer Erweiterung hinzugefügt

werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.
- Wenn ein Admin-Node oder Gateway-Node nur eingehenden Datenverkehr auf explizit konfigurierten Endpunkten annehmen soll, haben Sie die Load Balancer-Endpunkte definiert.



Vorhandene Client-Verbindungen können fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Schritte

1. Wählen Sie **Konfiguration > Netzwerkeinstellungen > Nicht Vertrauenswürdiges Clientnetzwerk**.

Die Seite nicht vertrauenswürdige Clientnetzwerke wird angezeigt.

Auf dieser Seite werden alle Knoten in Ihrem StorageGRID-System aufgelistet. Die Spalte „nicht verfügbar“ enthält einen Eintrag, wenn das Client-Netzwerk auf dem Knoten vertrauenswürdig sein muss.

Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as [load balancer endpoints](#).

Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network Default Trusted Untrusted

Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

<input type="checkbox"/>	Node Name	Unavailable Reason
<input type="checkbox"/>	DC1-ADM1	
<input type="checkbox"/>	DC1-G1	
<input type="checkbox"/>	DC1-S1	
<input type="checkbox"/>	DC1-S2	
<input type="checkbox"/>	DC1-S3	
<input type="checkbox"/>	DC1-S4	

Client Network untrusted on 0 nodes.

Save

2. Geben Sie im Abschnitt **Neue Knoten Standard** festlegen an, was die Standardeinstellung sein soll, wenn neue Knoten in einem Erweiterungsvorgang zum Raster hinzugefügt werden.

- **Trusted:** Wenn ein Knoten in einer Erweiterung hinzugefügt wird, wird seinem Client-Netzwerk vertraut.

- **UnTrusted:** Wenn ein Knoten in einer Erweiterung hinzugefügt wird, ist sein Client-Netzwerk nicht vertrauenswürdig. Sie können bei Bedarf zu dieser Seite zurückkehren, um die Einstellung für einen bestimmten neuen Knoten zu ändern.



Diese Einstellung hat keine Auswirkung auf die vorhandenen Nodes im StorageGRID System.

3. Wählen Sie im Abschnitt **nicht vertrauenswürdige Client-Netzwerkknoten auswählen** die Knoten aus, die Clientverbindungen nur auf explizit konfigurierten Load-Balancer-Endpunkten zulassen sollen.

Sie können das Kontrollkästchen im Titel auswählen oder deaktivieren, um alle Knoten auszuwählen oder zu deaktivieren.

4. Klicken Sie Auf **Speichern**.

Die neuen Firewall-Regeln werden sofort hinzugefügt und durchgesetzt. Vorhandene Client-Verbindungen können fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Verwandte Informationen

["Konfigurieren von Load Balancer-Endpunkten"](#)

Verwalten von Hochverfügbarkeitsgruppen

Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen) sorgen für hochverfügbare Datenverbindungen für S3 und Swift Clients. HA-Gruppen können auch für hochverfügbare Verbindungen mit dem Grid Manager und dem Tenant Manager verwendet werden.

- ["Eine HA-Gruppe"](#)
- ["Verwendung von HA-Gruppen"](#)
- ["Konfigurationsoptionen für HA-Gruppen"](#)
- ["Erstellen einer Hochverfügbarkeitsgruppe"](#)
- ["Bearbeiten einer Hochverfügbarkeitsgruppe"](#)
- ["Entfernen einer Hochverfügbarkeitsgruppe"](#)

Eine HA-Gruppe

Hochverfügbarkeitsgruppen verwenden virtuelle IP-Adressen (VIPs), um aktiv-Backup-Zugriff auf Gateway Node- oder Admin-Node-Services bereitzustellen.

Eine HA-Gruppe besteht aus mindestens einer Netzwerkschnittstellen an Admin-Nodes und Gateway-Nodes. 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.

Die aktive Schnittstelle in einer HA-Gruppe wird als Master bezeichnet. Alle anderen Schnittstellen werden als Backup bezeichnet. Um diese Bezeichnungen anzuzeigen, wählen Sie **Knoten > Node > Übersicht**.

DC1-ADM1 (Admin Node)

Overview Hardware Network Storage Load Balancer Events Tasks

Node Information ⓘ

Name	DC1-ADM1
Type	Admin Node
ID	711b7b9b-8d24-4d9f-877a-be3fa3ac27e8
Connection State	✔ Connected
Software Version	11.4.0 (build 20200515.2346.8edcbbf)
HA Groups	Fabric Pools, Master
IP Addresses	192.168.2.208, 10.224.2.208, 47.47.2.208, 47.47.4.219 Show more ▼

Beim Erstellen einer HA-Gruppe geben Sie eine Schnittstelle an, die der bevorzugte Master sein soll. Der bevorzugte Master ist die aktive Schnittstelle, wenn kein Fehler auftritt, der dazu führt, dass die VIP-Adressen einer Backup-Schnittstelle neu zugewiesen werden. Wenn der Fehler behoben ist, werden die VIP-Adressen automatisch zurück zum bevorzugten Master verschoben.

Ein Failover kann aus einem der folgenden Gründe ausgelöst werden:

- Der Node, auf dem die Schnittstelle konfiguriert ist, schaltet sich aus.
- Der Node, auf dem die Schnittstelle konfiguriert ist, verliert mindestens 2 Minuten lang die Verbindung zu allen anderen Nodes
- Die aktive Schnittstelle ausfällt.
- Der Lastverteiler-Dienst wird angehalten.
- Der High Availability Service stoppt.



Der Failover wird möglicherweise nicht durch Netzwerkausfälle außerhalb des Node ausgelöst, der die aktive Schnittstelle hostet. Ebenso wird der Failover nicht durch den Ausfall des CLB-Dienstes (veraltet) oder der Dienste für den Grid-Manager oder den Mandanten-Manager ausgelöst.

Wenn die HA-Gruppe Schnittstellen von mehr als zwei Nodes enthält, kann während des Failover die aktive Schnittstelle zu einer anderen Node verschoben werden.

Verwendung von HA-Gruppen

Es empfiehlt sich, aus mehreren Gründen Gruppen für Hochverfügbarkeit (HA) zu verwenden.

- Eine HA-Gruppe kann hochverfügbare administrative Verbindungen mit dem Grid Manager oder dem Mandanten Manager bereitstellen.
- Eine HA-Gruppe kann hochverfügbare Datenverbindungen für S3 und Swift Clients bieten.
- Eine HA-Gruppe, die nur eine Schnittstelle enthält, ermöglicht es Ihnen, viele VIP-Adressen bereitzustellen und explizit IPv6-Adressen festzulegen.

Eine HA-Gruppe kann nur Hochverfügbarkeit bieten, wenn alle Nodes in der Gruppe dieselben Services bereitstellen. Wenn Sie eine HA-Gruppe erstellen, fügen Sie Schnittstellen von den Typen von Nodes hinzu, die die erforderlichen Services bereitstellen.

- **Admin Nodes:** Schließen Sie den Load Balancer Service ein und ermöglichen Sie den Zugriff auf den Grid Manager oder den Tenant Manager.
- **Gateway-Knoten:** Schließen Sie den Load Balancer Service und den CLB-Dienst (veraltet) ein.

Zweck der HA-Gruppe	Fügen Sie diesem Typ Nodes der HA-Gruppe hinzu
Zugriff auf Grid Manager	<ul style="list-style-type: none"> • Primärer Admin-Node (bevorzugter Master) • Nicht primäre Admin-Nodes <p>Hinweis: der primäre Admin-Knoten muss der bevorzugte Master sein. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden.</p>
Zugriff nur auf Tenant Manager	<ul style="list-style-type: none"> • Primäre oder nicht primäre Admin-Nodes
S3- oder Swift-Client-Zugriff – Load Balancer Service	<ul style="list-style-type: none"> • Admin-Nodes • Gateway-Nodes
S3- oder Swift-Client-Zugriff — CLB-Service	<ul style="list-style-type: none"> • Gateway-Nodes <p>Hinweis: der CLB-Service ist veraltet.</p>

Einschränkungen bei der Verwendung von HA-Gruppen mit Grid Manager oder Tenant Manager

Der Ausfall von Services für den Grid Manager oder den Mandanten-Manager löst nicht ein Failover innerhalb der HA-Gruppe aus.

Wenn Sie sich bei einem Failover beim Grid Manager oder beim Tenant Manager angemeldet haben, werden Sie abgemeldet und müssen sich erneut anmelden, um Ihre Aufgabe fortzusetzen.

Einige Wartungsvorgänge können nicht ausgeführt werden, wenn der primäre Admin-Node nicht verfügbar ist. Während des Failovers können Sie Ihr StorageGRID-System mit dem Grid-Manager überwachen.

Einschränkungen bei der Verwendung von HA-Gruppen mit dem CLB-Service

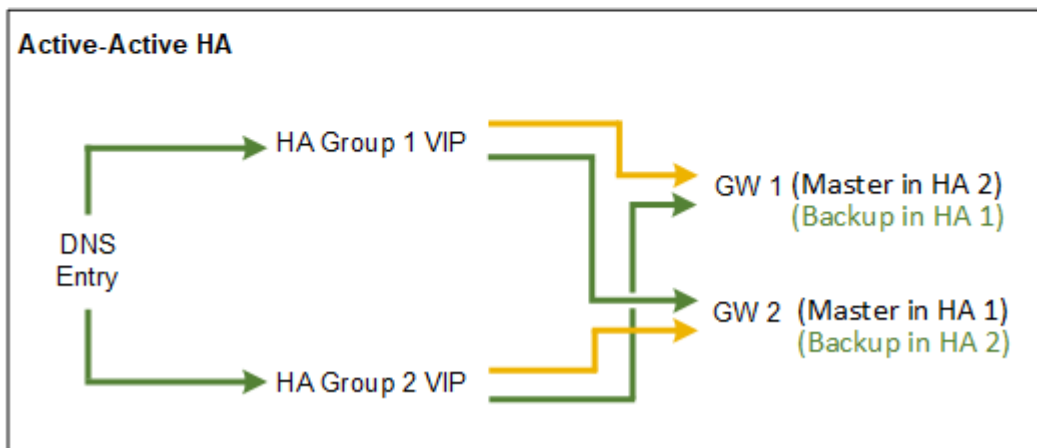
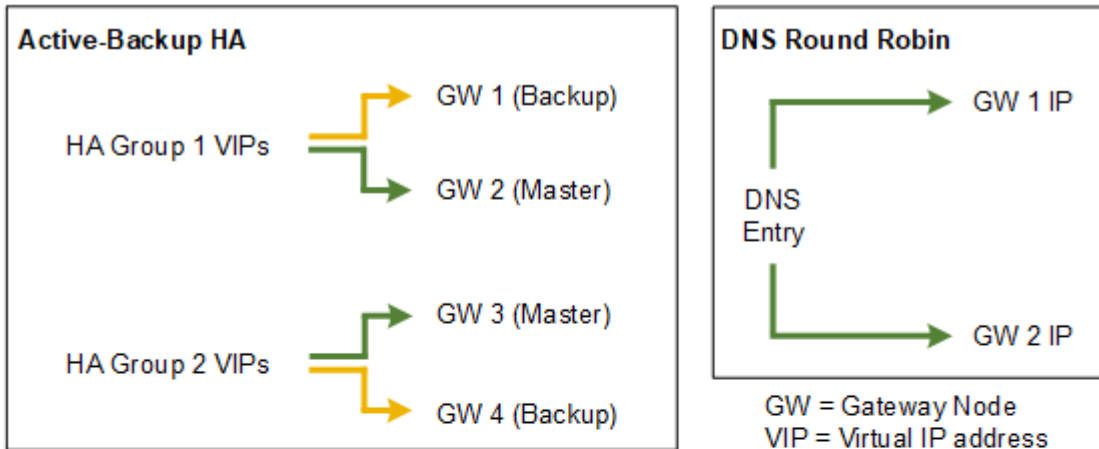
Der Ausfall des CLB-Dienstes löst nicht ein Failover innerhalb der HA-Gruppe aus.



Der CLB-Service ist veraltet.

Konfigurationsoptionen für HA-Gruppen

Die folgenden Diagramme bieten Beispiele für verschiedene Möglichkeiten zum Konfigurieren von HA-Gruppen. Jede Option hat vor- und Nachteile.



Wenn mehrere sich überschneidende HA-Gruppen erstellt werden, wie im „aktiv/aktiv-HA-Beispiel“ dargestellt, wird der Gesamtdurchsatz mit der Anzahl der Nodes und HA-Gruppen skaliert. Mit drei oder mehr Nodes und drei oder mehr HA-Gruppen können außerdem Vorgänge mithilfe einer der VIPs fortgesetzt werden – selbst bei Wartungsarbeiten, bei denen ein Node offline geschaltet werden muss.

Die Tabelle enthält eine Zusammenfassung der Vorteile der einzelnen HA-Konfigurationen, die in der Abbildung dargestellt sind.

Konfiguration	Vorteile	Nachteile
Aktiv/Backup HA	<ul style="list-style-type: none"> • Management über StorageGRID ohne externe Abhängigkeiten • Schnelles Failover. 	<ul style="list-style-type: none"> • In einer HA-Gruppe ist nur ein Node aktiv. Mindestens ein Node pro HA-Gruppe bleibt im Ruhezustand.

Konfiguration	Vorteile	Nachteile
DNS Round Robin	<ul style="list-style-type: none"> • Erhöhter Aggregatdurchsatz: • Keine leerlaufenden Hosts 	<ul style="list-style-type: none"> • Langsamer Failover, der vom Client-Verhalten abhängen kann. • Konfiguration von Hardware außerhalb von StorageGRID erforderlich • Benötigt eine vom Kunden implementierte Zustandsprüfung.
Aktiv/Aktiv	<ul style="list-style-type: none"> • Der Datenverkehr wird über mehrere HA-Gruppen verteilt. • Hoher Aggregatdurchsatz, der mit der Anzahl der HA-Gruppen skaliert werden kann • Schnelles Failover. 	<ul style="list-style-type: none"> • Komplexer zu konfigurieren. • Konfiguration von Hardware außerhalb von StorageGRID erforderlich • Benötigt eine vom Kunden implementierte Zustandsprüfung.

Erstellen einer Hochverfügbarkeitsgruppe

Sie können eine oder mehrere Hochverfügbarkeitsgruppen (HA-Gruppen) erstellen, die für hochverfügbaren Zugriff auf die Services in Admin-Nodes oder Gateway-Nodes sorgen.

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

Eine Schnittstelle muss die folgenden Bedingungen erfüllen, die in einer HA-Gruppe enthalten sein sollen:

- Die Schnittstelle muss für einen Gateway-Node oder einen Admin-Node verwendet werden.
- Die Schnittstelle muss zum Grid Network (eth0) oder dem Client Network (eth2) gehören.
- Die Schnittstelle muss mit fester oder statischer IP-Adresse konfiguriert werden, nicht mit DHCP.

Schritte

1. Wählen Sie **Konfiguration > Netzwerkeinstellungen > Hochverfügbarkeitsgruppen**.

Die Seite „Hochverfügbarkeitsgruppen“ wird angezeigt.

High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

+ Create ✎ Edit ✖ Remove

Name	Description	Virtual IP Addresses	Interfaces
<i>No HA groups found.</i>			

2. Klicken Sie Auf **Erstellen**.

Das Dialogfeld Gruppe für hohe Verfügbarkeit erstellen wird angezeigt.

3. Geben Sie einen Namen und, falls gewünscht, eine Beschreibung für die HA-Gruppe ein.

4. Klicken Sie Auf **Schnittstellen Auswählen**.

Das Dialogfeld Schnittstellen zu Hochverfügbarkeitsgruppe hinzufügen wird angezeigt. In der Tabelle werden die infrage kommenden Nodes, Schnittstellen und IPv4-Subnetze aufgeführt.

Add Interfaces to High Availability Group

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

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
	g140-g1	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g1	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g3	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g3	eth2	192.168.0.0/21	
	g140-g4	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g4	eth2	192.168.0.0/21	

There are 2 interfaces selected.

CancelApply

Eine Schnittstelle wird in der Liste nicht angezeigt, wenn ihre IP-Adresse durch DHCP zugewiesen wird.

5. Aktivieren Sie in der Spalte **zur HA-Gruppe** das Kontrollkästchen für die Schnittstelle, die zur HA-Gruppe hinzugefügt werden soll.

Beachten Sie die folgenden Richtlinien für die Auswahl von Schnittstellen:

- Sie müssen mindestens eine Schnittstelle auswählen.
- Wenn Sie mehrere Schnittstellen auswählen, müssen sich alle Schnittstellen entweder im Grid Network (eth0) oder im Client Network (eth2) befinden.
- Alle Schnittstellen müssen sich im gleichen Subnetz oder in Subnetzen mit einem gemeinsamen Präfix befinden.

IP-Adressen werden auf das kleinste Subnetz beschränkt (das mit dem größten Präfix).

- Wenn Sie Schnittstellen für verschiedene Node-Typen auswählen und ein Failover auftritt, sind nur die Dienste verfügbar, die für die ausgewählten Knoten gemeinsam sind.
 - Wählen Sie mindestens zwei Admin-Nodes aus, um den HA-Schutz des Grid Manager oder des Mandanten-Manager zu erhalten.
 - Wählen Sie zwei oder mehr Admin-Nodes, Gateway-Nodes oder beide aus, um den HA-Schutz des Load Balancer Service zu gewährleisten.
 - Wählen Sie mindestens zwei Gateway-Nodes aus, um den HA-Schutz des CLB-Service zu gewährleisten.



Der CLB-Service ist veraltet.

Add Interfaces to High Availability Group

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

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
<input checked="" type="checkbox"/>	DC1-ADM1	eth0	10.96.100.0/23	
<input checked="" type="checkbox"/>	DC1-G1	eth0	10.96.100.0/23	
<input checked="" type="checkbox"/>	DC2-ADM1	eth0	10.96.100.0/23	

There are 3 interfaces selected.

Attention: You have selected nodes of different types that run different services. If a failover occurs, only the services common to all node types will be available on the virtual IPs.

Cancel

Apply

6. Klicken Sie Auf **Anwenden**.

Die ausgewählten Schnittstellen werden auf der Seite Hochverfügbarkeitgruppe erstellen im Abschnitt Schnittstellen aufgeführt. Standardmäßig wird die erste Schnittstelle in der Liste als bevorzugter Master ausgewählt.

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
g140-g1	eth2	47.47.0.0/21	<input checked="" type="radio"/>
g140-g2	eth2	47.47.0.0/21	<input type="radio"/>

Displaying 2 interfaces.

Virtual IP Addresses

Virtual IP Subnet: 47.47.0.0/21. 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

7. Wenn Sie eine andere Schnittstelle als bevorzugten Master auswählen möchten, wählen Sie diese Schnittstelle in der Spalte **bevorzugter Master** aus.

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



Wenn die HA-Gruppe Zugriff auf den Grid Manager bietet, müssen Sie eine Schnittstelle am primären Admin-Node auswählen, um der bevorzugte Master-Typ zu sein. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden.

8. Geben Sie im Abschnitt virtuelle IP-Adressen der Seite eine bis 10 virtuelle IP-Adressen für die HA-Gruppe ein. Klicken Sie auf das Pluszeichen (+) Um mehrere IP-Adressen hinzuzufügen.

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

IPv4-Adressen müssen sich im IPv4-Subnetz befinden, das von allen Mitgliedschnittstellen gemeinsam

genutzt wird.

9. Klicken Sie Auf **Speichern**.

Die HA-Gruppe wird erstellt. Sie können jetzt die konfigurierten virtuellen IP-Adressen verwenden.

Verwandte Informationen

["Installieren Sie Red hat Enterprise Linux oder CentOS"](#)

["VMware installieren"](#)

["Installieren Sie Ubuntu oder Debian"](#)

["Managen des Lastausgleichs"](#)

Bearbeiten einer Hochverfügbarkeitsgruppe

Sie können eine HA-Gruppe (High Availability, Hochverfügbarkeit) bearbeiten, um ihren Namen und ihre Beschreibung zu ändern, Schnittstellen hinzuzufügen oder zu entfernen oder eine virtuelle IP-Adresse hinzuzufügen oder zu aktualisieren.

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

Das Bearbeiten einer HA-Gruppe hat einige der Gründe:

- Hinzufügen einer Schnittstelle zu einer vorhandenen Gruppe Die Schnittstellen-IP-Adresse muss sich innerhalb desselben Subnetzes befinden wie andere Schnittstellen, die der Gruppe bereits zugewiesen sind.
- Entfernen einer Schnittstelle aus einer HA-Gruppe. Sie können beispielsweise keine Deaktivierung eines Standorts oder Nodes starten, wenn die Schnittstelle eines Node für das Grid Network oder das Client Network in einer HA-Gruppe verwendet wird.

Schritte

1. Wählen Sie **Konfiguration > Netzwerkeinstellungen > Hochverfügbarkeitsgruppen**.

Die Seite „Hochverfügbarkeitsgruppen“ wird angezeigt.

High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

<input type="button" value="+ Create"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>				
	Name	Description	Virtual IP Addresses	Interfaces
<input type="radio"/>	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
<input type="radio"/>	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

Displaying 2 HA groups.

2. Wählen Sie die HA-Gruppe aus, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.

Das Dialogfeld „High Availability Group bearbeiten“ wird angezeigt.

3. Optional können Sie den Namen oder die Beschreibung der Gruppe aktualisieren.
4. Klicken Sie optional auf **Schnittstellen auswählen**, um die Schnittstellen für die HA-Gruppe zu ändern.

Das Dialogfeld Schnittstellen zu Hochverfügbarkeitsgruppe hinzufügen wird angezeigt.

Add Interfaces to High Availability Group

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

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
	g140-g1	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g1	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g3	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g3	eth2	192.168.0.0/21	
	g140-g4	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g4	eth2	192.168.0.0/21	

There are 2 interfaces selected.

Eine Schnittstelle wird in der Liste nicht angezeigt, wenn ihre IP-Adresse durch DHCP zugewiesen wird.

5. Aktivieren oder deaktivieren Sie die Kontrollkästchen, um Schnittstellen hinzuzufügen oder zu entfernen.

Beachten Sie die folgenden Richtlinien für die Auswahl von Schnittstellen:

- Sie müssen mindestens eine Schnittstelle auswählen.
- Wenn Sie mehrere Schnittstellen auswählen, müssen sich alle Schnittstellen entweder im Grid Network (eth0) oder im Client Network (eth2) befinden.

- Alle Schnittstellen müssen sich im gleichen Subnetz oder in Subnetzen mit einem gemeinsamen Präfix befinden.

IP-Adressen werden auf das kleinste Subnetz beschränkt (das mit dem größten Präfix).

- Wenn Sie Schnittstellen für verschiedene Node-Typen auswählen und ein Failover auftritt, sind nur die Dienste verfügbar, die für die ausgewählten Knoten gemeinsam sind.
 - Wählen Sie mindestens zwei Admin-Nodes aus, um den HA-Schutz des Grid Manager oder des Mandanten-Manager zu erhalten.
 - Wählen Sie zwei oder mehr Admin-Nodes, Gateway-Nodes oder beide aus, um den HA-Schutz des Load Balancer Service zu gewährleisten.
 - Wählen Sie mindestens zwei Gateway-Nodes aus, um den HA-Schutz des CLB-Service zu gewährleisten.



Der CLB-Service ist veraltet.

6. Klicken Sie Auf **Anwenden**.

Die ausgewählten Schnittstellen werden im Abschnitt Schnittstellen der Seite aufgeführt. Standardmäßig wird die erste Schnittstelle in der Liste als bevorzugter Master ausgewählt.

Edit High Availability Group 'HA Group - Admin Nodes'

High Availability Group

Name

Description

Interfaces

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

Node Name	Interface	IPv4 Subnet	Preferred Master
DC1-ADM1	eth0	10.96.100.0/23	<input checked="" type="radio"/>
DC2-ADM1	eth0	10.96.100.0/23	<input type="radio"/>

Displaying 2 interfaces.

Virtual IP Addresses

Virtual IP Subnet: 10.96.100.0/23. 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

7. Wenn Sie eine andere Schnittstelle als bevorzugten Master auswählen möchten, wählen Sie diese Schnittstelle in der Spalte **bevorzugter Master** aus.

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



Wenn die HA-Gruppe Zugriff auf den Grid Manager bietet, müssen Sie eine Schnittstelle am primären Admin-Node auswählen, um der bevorzugte Master-Typ zu sein. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden.

8. Optional können Sie die virtuellen IP-Adressen für die HA-Gruppe aktualisieren.

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

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

9. Klicken Sie Auf **Speichern**.

Die HA-Gruppe wird aktualisiert.

Entfernen einer Hochverfügbarkeitsgruppe

Sie können eine HA-Gruppe (High Availability, Hochverfügbarkeit) entfernen, die Sie nicht mehr verwenden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Diese Aufgabe auslassen

Wenn Sie eine HA-Gruppe entfernen, können alle S3- oder Swift-Clients, die für die Verwendung einer der virtuellen IP-Adressen der Gruppe konfiguriert sind, keine Verbindung zu StorageGRID mehr herstellen. Um Client-Unterbrechungen zu vermeiden, sollten Sie alle betroffenen S3 oder Swift Client-Applikationen aktualisieren, bevor Sie eine HA-Gruppe entfernen. Aktualisieren Sie jeden Client, um eine Verbindung über eine andere IP-Adresse herzustellen, z. B. die virtuelle IP-Adresse einer anderen HA-Gruppe oder die IP-Adresse, die während der Installation oder bei der Verwendung von DHCP für eine Schnittstelle konfiguriert wurde.

Schritte

1. Wählen Sie **Konfiguration > Netzwerkeinstellungen > Hochverfügbarkeitsgruppen**.

Die Seite „Hochverfügbarkeitsgruppen“ wird angezeigt.

High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

	Name	Description	Virtual IP Addresses	Interfaces
<input type="radio"/>	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
<input type="radio"/>	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

Displaying 2 HA groups.

2. Wählen Sie die HA-Gruppe aus, die Sie entfernen möchten, und klicken Sie auf **Entfernen**.

Die Warnung „Gruppe mit hoher Verfügbarkeit löschen“ wird angezeigt.

Warning

Delete High Availability Group

Are you sure you want to delete High Availability Group 'HA group 1'?

Cancel

OK

3. Klicken Sie auf **OK**.

Die HA-Gruppe wird entfernt.

Konfigurieren von S3-API-Endpunkt-Domain-Namen

Um virtuelle S3-Hosted-Style-Anforderungen zu unterstützen, müssen Sie die Liste der Endpunkt-Domain-Namen, mit denen S3-Clients verbunden werden, mit konfigurieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen bestätigt haben, dass ein Grid-Upgrade nicht ausgeführt wird.



Nehmen Sie keine Änderungen an der Domänennamenkonfiguration vor, wenn ein Grid-Upgrade ausgeführt wird.

Über diese Aufgabe

Damit Clients S3-Endpunkt-Domain-Namen verwenden können, müssen Sie alle der folgenden Aufgaben ausführen:

- Verwenden Sie den Grid-Manager, um dem StorageGRID System die S3-Endpunkt-Domain-Namen hinzuzufügen.
- Stellen Sie sicher, dass das Zertifikat, das der Client für HTTPS-Verbindungen zu StorageGRID verwendet, für alle vom Client erforderlichen Domänennamen signiert ist.

Beispiel: Wenn der Endpunkt lautet `s3.company.com`, Sie müssen sicherstellen, dass das Zertifikat verwendet für HTTPS-Verbindungen enthält die `s3.company.com` endpoint und Wildcard-alternativer Name (SAN) des Endpunkts: `*.s3.company.com`.

- Konfigurieren Sie den vom Client verwendeten DNS-Server. Fügen Sie DNS-Datensätze für die IP-Adressen ein, die von Clients zum Herstellen von Verbindungen verwendet werden, und stellen Sie sicher, dass die Datensätze auf alle erforderlichen Endpunkt-Domänennamen verweisen, einschließlich Platzhalternamen.



Clients können sich mit StorageGRID über die IP-Adresse eines Gateway-Node, eines Admin-Nodes oder eines Storage-Nodes oder durch Verbindung mit der virtuellen IP-Adresse einer Hochverfügbarkeitsgruppe verbinden. Sie sollten verstehen, wie Client-Anwendungen eine Verbindung zum Raster herstellen, sodass Sie die richtigen IP-Adressen in die DNS-Einträge aufnehmen können.

Das Zertifikat, das ein Client für HTTPS-Verbindungen verwendet, hängt davon ab, wie der Client mit dem Grid verbindet:

- Wenn ein Client eine Verbindung über den Load Balancer-Service herstellt, verwendet er das Zertifikat für einen bestimmten Load Balancer-Endpunkt.



Jeder Load Balancer-Endpunkt verfügt über ein eigenes Zertifikat, und jeder Endpunkt kann so konfiguriert werden, dass verschiedene Endpunkt-Domain-Namen erkannt werden.

- Wenn der Client eine Verbindung zu einem Storage-Node oder zum CLB-Dienst auf einem Gateway-Node herstellt, verwendet der Client ein benutzerdefiniertes Grid-Serverzertifikat, das aktualisiert wurde, um alle erforderlichen Endpunkt-Domännennamen einzuschließen.



Der CLB-Service ist veraltet.

Schritte

1. Wählen Sie **Konfiguration > Netzwerkeinstellungen > Domännennamen**.

Die Seite „Endpoint Domain-Namen“ wird angezeigt.

Endpoint Domain Names

Virtual Hosted-Style Requests

Enable support of S3 virtual hosted-style requests by specifying API endpoint domain names. Support is disabled if this list is empty. Examples: s3.example.com, s3.example.co.uk, s3-east.example.com

Endpoint 1	<input type="text" value="s3.example.com"/>	✕
Endpoint 2	<input type="text"/>	+ ✕

2. Geben Sie mit dem (+)-Symbol die Liste der S3-API-Endpunktdomännennamen in die Felder **Endpunkt** ein.

Wenn diese Liste leer ist, ist die Unterstützung für virtuelle S3-Hosted-Style-Anforderungen deaktiviert.

3. Klicken Sie Auf **Speichern**.

4. Stellen Sie sicher, dass die Serverzertifikate, die Clients verwenden, mit den erforderlichen Endpunktdomännennamen übereinstimmen.
 - Aktualisieren Sie für Clients, die den Lastverteilungsdienst verwenden, das Zertifikat, das dem Lastausgleichsendpunkt zugeordnet ist, mit dem der Client verbunden ist.
 - Aktualisieren Sie für Clients, die eine direkte Verbindung zu Speicherknoten herstellen oder den CLB-Dienst auf Gateway-Knoten verwenden, das benutzerdefinierte Serverzertifikat für das Grid.

5. Fügen Sie die erforderlichen DNS-Einträge hinzu, um sicherzustellen, dass die Anforderungen für den Domännennamen des Endpunkts aufgelöst werden können.

Ergebnis

Wenn Clients nun den Endpunkt verwenden `bucket.s3.company.com`, Der DNS-Server löst sich auf den richtigen Endpunkt und das Zertifikat authentifiziert den Endpunkt wie erwartet.

Verwandte Informationen

["S3 verwenden"](#)

["Anzeigen von IP-Adressen"](#)

["Erstellen einer Hochverfügbarkeitsgruppe"](#)

["Konfigurieren eines benutzerdefinierten Serverzertifikats für Verbindungen mit dem Speicherknoten oder dem CLB-Dienst"](#)

["Konfigurieren von Load Balancer-Endpunkten"](#)

Aktivieren von HTTP für die Clientkommunikation

Standardmäßig verwenden Client-Anwendungen das HTTPS-Netzwerkprotokoll für alle Verbindungen zu Storage-Nodes oder zum veralteten CLB-Dienst auf Gateway-Nodes. Optional können Sie HTTP für diese Verbindungen aktivieren, z. B. beim Testen eines nicht produktiven Grids.

Was Sie benötigen

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

Über diese Aufgabe

Führen Sie diese Aufgabe nur aus, wenn S3- und Swift-Clients HTTP-Verbindungen direkt zu Storage-Nodes oder zum veralteten CLB-Service auf Gateway-Nodes herstellen müssen.

Sie müssen diese Aufgabe nicht für Clients abschließen, die nur HTTPS-Verbindungen verwenden oder für Clients, die eine Verbindung zum Load Balancer-Dienst herstellen (da Sie jeden Load Balancer-Endpunkt so konfigurieren können, dass entweder HTTP oder HTTPS verwendet werden). Weitere Informationen finden Sie in den Informationen zum Konfigurieren von Load Balancer-Endpunkten.

Siehe ["Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen"](#) Um zu erfahren, welche S3- und Swift-Clients beim Herstellen einer Verbindung zu Storage-Nodes oder zum veralteten CLB-Dienst über HTTP oder HTTPS verwenden



Gehen Sie vorsichtig vor, wenn Sie HTTP für ein Produktions-Grid aktivieren, da die Anforderungen unverschlüsselt gesendet werden.

Schritte

1. Wählen Sie **Konfiguration > Systemeinstellungen > Gitteroptionen**.
2. Aktivieren Sie im Abschnitt Netzwerkooptionen das Kontrollkästchen **HTTP-Verbindung aktivieren**.

Network Options

Prevent Client Modification  

Enable HTTP Connection 

Network Transfer Encryption  AES128-SHA AES256-SHA

3. Klicken Sie Auf **Speichern**.

Verwandte Informationen

["Konfigurieren von Load Balancer-Endpunkten"](#)

["S3 verwenden"](#)

["Verwenden Sie Swift"](#)

Steuern, welche Client-Operationen zulässig sind

Sie können die Option „Client Modification Grid verhindern“ auswählen, um bestimmte HTTP-Client-Vorgänge zu verweigern.

Was Sie benötigen

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

Über diese Aufgabe

„Client-Änderung verhindern“ ist eine systemweite Einstellung. Wenn die Option „Client-Änderung verhindern“ ausgewählt ist, werden die folgenden Anfragen verweigert:

• S3 REST API

- Bucket-Anforderungen löschen
- Alle Anforderungen, die das Ändern von Daten eines vorhandenen Objekts, benutzerdefinierter Metadaten oder S3-Objekt-Tagging zum Einsatz kommen



Diese Einstellung gilt nicht für Buckets mit aktivierter Versionierung. Bei der Versionierung werden bereits Änderungen an Objektdaten, benutzerdefinierten Metadaten und Objekt-Tagging verhindert.

• Swift REST API

- Container-Anforderungen löschen
- Anträge zum Ändern vorhandener Objekte. Beispielsweise werden folgende Vorgänge verweigert: Put Overwrite, Delete, Metadata Update usw.

Schritte

1. Wählen Sie **Konfiguration > Systemeinstellungen > Gitteroptionen**.

2. Aktivieren Sie im Abschnitt Netzwerkoptionen das Kontrollkästchen **Client-Änderung verhindern**.

Network Options

Prevent Client Modification



Enable HTTP Connection



Network Transfer Encryption



AES128-SHA

AES256-SHA

3. Klicken Sie Auf **Speichern**.

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.