Konfigurieren von Clientverbindungen

StorageGRID software

NetApp
October 21, 2025

Inhalt

Konfigurieren von Clientverbindungen

Konfigurieren von S3-Clientverbindungen

Als Grid-Administrator verwalten Sie die Konfigurationsoptionen, die steuern, wie S3-Clientanwendungen eine Verbindung zu Ihrem StorageGRID -System herstellen, um Daten zu speichern und abzurufen.

Swift-Details wurden aus dieser Version der Dokumentationssite entfernt. Sehen "StorageGRID 11.8: S3- und Swift-Clientverbindungen konfigurieren" .

Konfigurationsaufgaben

1. Führen Sie die erforderlichen Aufgaben in StorageGRID aus, je nachdem, wie die Clientanwendung eine Verbindung zu StorageGRID herstellt.

Erforderliche Aufgaben

Sie müssen Folgendes besorgen:

- IP-Adressen
- Domänennamen
- SSL-Zertifikat

Optionale Aufgaben

Konfigurieren Sie optional:

- Identitätsföderation
- SSO

1. Verwenden Sie StorageGRID , um die Werte abzurufen, die die Anwendung für die Verbindung mit dem Grid benötigt. Sie können entweder den S3-Setup-Assistenten verwenden oder jede StorageGRID Einheit manuell konfigurieren.

Verwenden Sie den S3-Setup-Assistenten

Befolgen Sie die Schritte im S3-Setup-Assistenten.

Manuell konfigurieren

1. Erstellen einer Hochverfügbarkeitsgruppe
2. Erstellen eines Load Balancer-Endpunkts
3. Mieterkonto erstellen
4. Bucket und Zugriffsschlüssel erstellen
5. Konfigurieren der ILM-Regel und -Richtlinie

1. Verwenden Sie die S3-Anwendung, um die Verbindung zu StorageGRID herzustellen. Erstellen Sie DNS-

Einträge, um IP-Adressen den Domänennamen zuzuordnen, die Sie verwenden möchten.

Führen Sie bei Bedarf zusätzliche Anwendungseinstellungen durch.

2. Führen Sie laufende Aufgaben in der Anwendung und in StorageGRID aus, um den Objektspeicher im Laufe der Zeit zu verwalten und zu überwachen.

Erforderliche Informationen zum Anhängen von StorageGRID an eine Clientanwendung

Bevor Sie StorageGRID an eine S3-Clientanwendung anhängen können, müssen Sie Konfigurationsschritte in StorageGRID ausführen und bestimmte Werte abrufen.

Welche Werte benötige ich?

Die folgende Tabelle zeigt die Werte, die Sie in StorageGRID konfigurieren müssen, und wo diese Werte von der S3-Anwendung und dem DNS-Server verwendet werden.

Wert	Wo der Wert konfiguriert ist	Wo Wert verwendet wird
Virtuelle IP-Adressen (VIP)	StorageGRID > HA-Gruppe	DNS-Eintrag
Hafen	StorageGRID > Load Balancer-Endpunkt	Client-Anwendung
SSL-Zertifikat	StorageGRID > Load Balancer-Endpunkt	Client-Anwendung
Servername (FQDN)	StorageGRID > Load Balancer-Endpunkt	• Client-Anwendung • DNS-Eintrag
S3-Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel	StorageGRID > Mandant und Bucket	Client-Anwendung
Bucket-/Containername	StorageGRID > Mandant und Bucket	Client-Anwendung

Wie komme ich an diese Werte?

Je nach Ihren Anforderungen können Sie die benötigten Informationen auf folgende Weise abrufen:

- *Verwenden Sie die"S3-Setup-Assistent" *. Der S3-Setup-Assistent hilft Ihnen, die erforderlichen Werte in StorageGRID schnell zu konfigurieren und gibt ein oder zwei Dateien aus, die Sie bei der Konfiguration der S3-Anwendung verwenden können. Der Assistent führt Sie durch die erforderlichen Schritte und hilft sicherzustellen, dass Ihre Einstellungen den Best Practices von StorageGRID entsprechen.

> Wenn Sie eine S3-Anwendung konfigurieren, wird die Verwendung des S3-Setup-Assistenten empfohlen, es sei denn, Sie wissen, dass Sie besondere Anforderungen haben oder Ihre Implementierung erhebliche Anpassungen erfordert.

- *Verwenden Sie die"FabricPool -Setup-Assistent" *. Ähnlich wie der S3-Setup-Assistent hilft Ihnen der FabricPool -Setup-Assistent dabei, die erforderlichen Werte schnell zu konfigurieren und gibt eine Datei aus, die Sie beim Konfigurieren einer FabricPool Cloud-Ebene in ONTAP verwenden können.

> ⓘ Wenn Sie StorageGRID als Objektspeichersystem für eine FabricPool Cloud-Ebene verwenden möchten, wird die Verwendung des FabricPool -Setup-Assistenten empfohlen, es sei denn, Sie wissen, dass Sie besondere Anforderungen haben oder Ihre Implementierung erhebliche Anpassungen erfordert.

- **Elemente manuell konfigurieren**. Wenn Sie eine Verbindung zu einer S3-Anwendung herstellen und den S3-Setup-Assistenten nicht verwenden möchten, können Sie die erforderlichen Werte erhalten, indem Sie die Konfiguration manuell durchführen. Gehen Sie folgendermaßen vor:
  a. Konfigurieren Sie die Hochverfügbarkeitsgruppe (HA), die Sie für die S3-Anwendung verwenden möchten. Sehen "Konfigurieren von Hochverfügbarkeitsgruppen" .
  b. Erstellen Sie den Load Balancer-Endpunkt, den die S3-Anwendung verwenden wird. Sehen "Konfigurieren von Load Balancer-Endpunkten" .
  c. Erstellen Sie das Mandantenkonto, das die S3-Anwendung verwenden wird. Sehen "Erstellen Sie ein Mieterkonto" .
  d. Melden Sie sich bei einem S3-Mandanten beim Mandantenkonto an und generieren Sie eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel für jeden Benutzer, der auf die Anwendung zugreift. Sehen "Erstellen Sie Ihre eigenen Zugriffsschlüssel" .
  e. Erstellen Sie einen oder mehrere S3-Buckets innerhalb des Mandantenkontos. Für S3 siehe"S3-Bucket erstellen" .
  f. Um spezifische Platzierungsanweisungen für die Objekte hinzuzufügen, die zum neuen Mandanten oder Bucket/Container gehören, erstellen Sie eine neue ILM-Regel und aktivieren Sie eine neue ILM-Richtlinie, um diese Regel zu verwenden. Sehen"ILM-Regel erstellen" Und"ILM-Richtlinie erstellen" .

Sicherheit für S3-Clients

StorageGRID Mandantenkonten verwenden S3-Clientanwendungen, um Objektdaten in StorageGRID zu speichern. Sie sollten die für Clientanwendungen implementierten Sicherheitsmaßnahmen überprüfen.

Zusammenfassung

Die folgende Liste fasst zusammen, wie die Sicherheit für die S3 REST API implementiert wird:

Verbindungssicherheit
TLS

Serverauthentifizierung
Von der Systemzertifizierungsstelle signiertes X.509-Serverzertifikat oder vom Administrator bereitgestelltes benutzerdefiniertes Serverzertifikat

Client-Authentifizierung
S3-Kontozugriffsschlüssel-ID und geheimer Zugriffsschlüssel

Client-Autorisierung

Bucket-Eigentümerschaft und alle geltenden Zugriffskontrollrichtlinien

So bietet StorageGRID Sicherheit für Clientanwendungen

S3-Clientanwendungen können eine Verbindung zum Load Balancer-Dienst auf Gateway-Knoten oder Admin-Knoten oder direkt zu Speicherknoten herstellen.

- Clients, die eine Verbindung zum Load Balancer-Dienst herstellen, können HTTPS oder HTTP verwenden, je nachdem, wie Sie"Konfigurieren Sie den Load Balancer-Endpunkt" .

  HTTPS bietet eine sichere, TLS-verschlüsselte Kommunikation und wird empfohlen. Sie müssen dem Endpunkt ein Sicherheitszertifikat beifügen.

  HTTP bietet eine weniger sichere, unverschlüsselte Kommunikation und sollte nur für Nicht-Produktions- oder Test-Grids verwendet werden.

- Clients, die eine Verbindung zu Speicherknoten herstellen, können auch HTTPS oder HTTP verwenden.

  HTTPS ist die Standardeinstellung und wird empfohlen.

  HTTP bietet eine weniger sichere, unverschlüsselte Kommunikation, kann aber optional"ermöglicht" für Nicht-Produktions- oder Testnetze.

- Die Kommunikation zwischen StorageGRID und dem Client wird mit TLS verschlüsselt.
- Die Kommunikation zwischen dem Load Balancer-Dienst und den Speicherknoten innerhalb des Grids wird verschlüsselt, unabhängig davon, ob der Load Balancer-Endpunkt für die Annahme von HTTP- oder HTTPS-Verbindungen konfiguriert ist.
- Kunden müssen liefern"HTTP-Authentifizierungsheader" zu StorageGRID , um REST-API-Operationen durchzuführen.

Sicherheitszertifikate und Clientanwendungen

In allen Fällen können Clientanwendungen TLS-Verbindungen herstellen, indem sie entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein vom StorageGRID System generiertes Zertifikat verwenden:

- Wenn Clientanwendungen eine Verbindung zum Load Balancer-Dienst herstellen, verwenden sie das Zertifikat, das für den Load Balancer-Endpunkt konfiguriert wurde. Jeder Load Balancer-Endpunkt verfügt über ein eigenes Zertifikat – entweder ein benutzerdefiniertes Serverzertifikat, das vom Grid-Administrator hochgeladen wurde, oder ein Zertifikat, das der Grid-Administrator beim Konfigurieren des Endpunkts in StorageGRID generiert hat.

  Sehen "Überlegungen zum Lastenausgleich" .

- Wenn Clientanwendungen eine direkte Verbindung zu einem Speicherknoten herstellen, verwenden sie entweder die vom System generierten Serverzertifikate, die bei der Installation des StorageGRID -Systems für Speicherknoten generiert wurden (und von der Systemzertifizierungsstelle signiert sind), oder ein einzelnes benutzerdefiniertes Serverzertifikat, das von einem Grid-Administrator für das Grid bereitgestellt wird. Sehen "Fügen Sie ein benutzerdefiniertes S3-API-Zertifikat hinzu" .

Clients sollten so konfiguriert werden, dass sie der Zertifizierungsstelle vertrauen, die das von ihnen zum Herstellen von TLS-Verbindungen verwendete Zertifikat signiert hat.

Unterstützte Hashing- und Verschlüsselungsalgorithmen für TLS-Bibliotheken

Das StorageGRID -System unterstützt eine Reihe von Verschlüsselungssammlungen, die Clientanwendungen beim Herstellen einer TLS-Sitzung verwenden können. Um Verschlüsselungen zu konfigurieren, gehen Sie zu **KONFIGURATION** > **Sicherheit** > **Sicherheitseinstellungen** und wählen Sie **TLS- und SSH-Richtlinien**.

Unterstützte Versionen von TLS

StorageGRID unterstützt TLS 1.2 und TLS 1.3.

SSLv3 und TLS 1.1 (oder frühere Versionen) werden nicht mehr unterstützt.

Verwenden Sie den S3-Setup-Assistenten

S3-Setup-Assistent verwenden: Überlegungen und Anforderungen

Sie können den S3-Setup-Assistenten verwenden, um StorageGRID als Objektspeichersystem für eine S3-Anwendung zu konfigurieren.

Wann Sie den S3-Setup-Assistenten verwenden sollten

Der S3-Setup-Assistent führt Sie durch jeden Schritt der Konfiguration von StorageGRID für die Verwendung mit einer S3-Anwendung. Beim Abschließen des Assistenten laden Sie Dateien herunter, mit denen Sie Werte in die S3-Anwendung eingeben können. Verwenden Sie den Assistenten, um Ihr System schneller zu konfigurieren und sicherzustellen, dass Ihre Einstellungen den Best Practices von StorageGRID entsprechen.

Wenn Sie die"Root-Zugriffsberechtigung" : Sie können den S3-Setup-Assistenten abschließen, wenn Sie mit der Verwendung des StorageGRID Grid Managers beginnen, oder Sie können zu einem späteren Zeitpunkt auf den Assistenten zugreifen und ihn abschließen. Je nach Bedarf können Sie auch einige oder alle benötigten Elemente manuell konfigurieren und anschließend mit dem Assistenten die Werte zusammenstellen, die eine S3-Anwendung benötigt.

Vor der Verwendung des Assistenten

Bevor Sie den Assistenten verwenden, vergewissern Sie sich, dass Sie diese Voraussetzungen erfüllt haben.

Beziehen Sie IP-Adressen und richten Sie VLAN-Schnittstellen ein

Wenn Sie eine Hochverfügbarkeitsgruppe (HA) konfigurieren, wissen Sie, mit welchen Knoten die S3-Anwendung eine Verbindung herstellt und welches StorageGRID Netzwerk verwendet wird. Sie wissen auch, welche Werte Sie für das Subnetz-CIDR, die Gateway-IP-Adresse und die virtuellen IP-Adressen (VIP) eingeben müssen.

Wenn Sie ein virtuelles LAN verwenden möchten, um den Datenverkehr von der S3-Anwendung zu trennen, haben Sie die VLAN-Schnittstelle bereits konfiguriert. Sehen "Konfigurieren von VLAN-Schnittstellen" .

Konfigurieren der Identitätsföderation und SSO

Wenn Sie Identitätsföderation oder Single Sign-On (SSO) für Ihr StorageGRID System verwenden möchten, haben Sie diese Funktionen aktiviert. Sie wissen auch, welche föderierte Gruppe Root-Zugriff auf das Mandantenkonto haben sollte, das die S3-Anwendung verwenden wird. Sehen"Verwenden der Identitätsföderation" Und"Konfigurieren der einmaligen Anmeldung" .

Domänennamen abrufen und konfigurieren

Sie wissen, welchen vollqualifizierten Domänennamen (FQDN) Sie für StorageGRID verwenden müssen. Einträge des Domänennamenservers (DNS) ordnen diesen FQDN den virtuellen IP-Adressen (VIP) der HA-Gruppe zu, die Sie mit dem Assistenten erstellen.

Wenn Sie virtuelle S3-Hosting-Anfragen verwenden möchten, sollten Sie"konfigurierte S3-Endpunktdomänennamen" . Es wird empfohlen, Anfragen im virtuellen gehosteten Stil zu verwenden.

Überprüfen Sie die Anforderungen für Load Balancer und Sicherheitszertifikate

Wenn Sie den StorageGRID Lastenausgleich verwenden möchten, haben Sie die allgemeinen Überlegungen zum Lastenausgleich überprüft. Sie verfügen über die Zertifikate, die Sie hochladen möchten, oder über die Werte, die Sie zum Generieren eines Zertifikats benötigen.

Wenn Sie einen externen Load Balancer-Endpunkt (eines Drittanbieters) verwenden möchten, verfügen Sie über den vollqualifizierten Domänennamen (FQDN), den Port und das Zertifikat für diesen Load Balancer.

Konfigurieren Sie alle Grid-Föderation-Verbindungen

Wenn Sie dem S3-Mandanten das Klonen von Kontodaten und das Replizieren von Bucket-Objekten in ein anderes Grid mithilfe einer Grid-Föderationsverbindung erlauben möchten, bestätigen Sie Folgendes, bevor Sie den Assistenten starten:

- Du hast"die Grid-Föderation-Verbindung konfiguriert" .
- Der Status der Verbindung ist **Verbunden**.
- Sie verfügen über Root-Zugriffsberechtigung.

Greifen Sie auf den S3-Setup-Assistenten zu und schließen Sie ihn ab

Sie können den S3-Setup-Assistenten verwenden, um StorageGRID für die Verwendung mit einer S3-Anwendung zu konfigurieren. Der Setup-Assistent stellt die Werte bereit, die die Anwendung benötigt, um auf einen StorageGRID Bucket zuzugreifen und Objekte zu speichern.

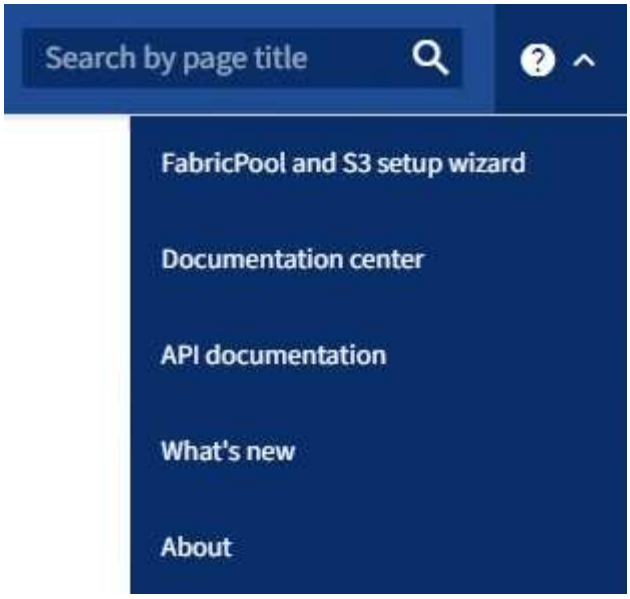
Bevor Sie beginnen

- Sie haben die"Root-Zugriffsberechtigung" .
- Sie haben die"Überlegungen und Anforderungen" zur Verwendung des Assistenten.

Zugriff auf den Assistenten

Schritte

1. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .
2. Wenn das Banner * FabricPool und S3-Setup-Assistent* auf dem Dashboard angezeigt wird, wählen Sie den Link im Banner aus. Wenn das Banner nicht mehr angezeigt wird, wählen Sie das Hilfesymbol in der Kopfzeile im Grid Manager und wählen Sie * FabricPool und S3-Setup-Assistent*.



3. Wählen Sie im Abschnitt „S3-Anwendung“ der Seite des FabricPool und S3-Setup-Assistenten die Option „Jetzt konfigurieren“ aus.

Schritt 1 von 6: HA-Gruppe konfigurieren

Eine HA-Gruppe ist eine Sammlung von Knoten, die jeweils den StorageGRID Load Balancer-Dienst enthalten. Eine HA-Gruppe kann Gateway-Knoten, Admin-Knoten oder beides enthalten.

Sie können eine HA-Gruppe verwenden, um die Verfügbarkeit der S3-Datenverbindungen aufrechtzuerhalten. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle die Arbeitslast mit geringen Auswirkungen auf den S3-Betrieb verwalten.

Einzelheiten zu dieser Aufgabe finden Sie unter"Verwalten von Hochverfügbarkeitsgruppen" .

Schritte

1. Wenn Sie einen externen Lastenausgleich verwenden möchten, müssen Sie keine HA-Gruppe erstellen. Wählen Sie **Diesen Schritt überspringen** und gehen Sie zuSchritt 2 von 6: Load Balancer-Endpunkt konfigurieren .
2. Um den StorageGRID Load Balancer zu verwenden, können Sie eine neue HA-Gruppe erstellen oder eine vorhandene HA-Gruppe verwenden.

HA-Gruppe erstellen

a. Um eine neue HA-Gruppe zu erstellen, wählen Sie **HA-Gruppe erstellen**.

b. Füllen Sie für den Schritt **Details eingeben** die folgenden Felder aus.

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

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

Nutzen Sie die Spaltenüberschriften zum Sortieren der Zeilen oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.

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

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

Ziehen Sie Zeilen, um die Werte in der Spalte **Prioritätsreihenfolge** zu ändern.

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

Wenn die HA-Gruppe mehr als eine Schnittstelle umfasst und die aktive Schnittstelle ausfällt, werden die virtuellen IP-Adressen (VIP) zur ersten Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. Wenn diese Schnittstelle ausfällt, werden die VIP-Adressen zur nächsten Backup-Schnittstelle verschoben und so weiter. Wenn die Fehler behoben sind, werden die VIP-Adressen wieder an die Schnittstelle mit der höchsten verfügbaren Priorität weitergeleitet.

e. Füllen Sie für den Schritt **IP-Adressen eingeben** die folgenden Felder aus.

Feld	Beschreibung
Subnetz-CIDR	Die Adresse des VIP-Subnetzes in CIDR-Notation – eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetzlänge (0-32). Für die Netzwerkadresse dürfen keine Hostbits gesetzt sein. Beispiel: `192.16.0.0/22`.
Gateway-IP-Adresse (optional)	Wenn sich die für den Zugriff auf StorageGRID verwendeten S3-IP-Adressen nicht im selben Subnetz wie die StorageGRID VIP-Adressen befinden, geben Sie die lokale Gateway-IP-Adresse des StorageGRID VIP ein. Die lokale Gateway-IP-Adresse muss sich innerhalb des VIP-Subnetzes befinden.

Feld	Beschreibung
Virtuelle IP-Adresse	Geben Sie mindestens eine und höchstens zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden. Mindestens eine Adresse muss IPv4 sein. Optional können Sie zusätzliche IPv4- und IPv6-Adressen angeben.

f. Wählen Sie **HA-Gruppe erstellen** und dann **Fertig stellen**, um zum S3-Setup-Assistenten zurückzukehren.

g. Wählen Sie **Weiter**, um zum Schritt „Lastenausgleich“ zu gelangen.

Vorhandene HA-Gruppe verwenden

a. Um eine vorhandene HA-Gruppe zu verwenden, wählen Sie den Namen der HA-Gruppe aus der Liste **HA-Gruppe auswählen** aus.

b. Wählen Sie **Weiter**, um zum Schritt „Lastenausgleich“ zu gelangen.

Schritt 2 von 6: Load Balancer-Endpunkt konfigurieren

StorageGRID verwendet einen Load Balancer, um die Arbeitslast von Clientanwendungen zu verwalten. Durch Lastenausgleich werden Geschwindigkeit und Verbindungskapazität über mehrere Speicherknoten hinweg maximiert.

Sie können den StorageGRID Load Balancer-Dienst verwenden, der auf allen Gateway- und Admin-Knoten vorhanden ist, oder Sie können eine Verbindung zu einem externen Load Balancer (eines Drittanbieters) herstellen. Die Verwendung des StorageGRID Load Balancers wird empfohlen.

Einzelheiten zu dieser Aufgabe finden Sie unter"Überlegungen zum Lastenausgleich" .

Um den StorageGRID Load Balancer-Dienst zu verwenden, wählen Sie die Registerkarte * StorageGRID Load Balancer* und erstellen oder wählen Sie dann den Load Balancer-Endpunkt aus, den Sie verwenden möchten. Um einen externen Lastenausgleich zu verwenden, wählen Sie die Registerkarte **Externer Lastenausgleich** und geben Sie Details zu dem System an, das Sie bereits konfiguriert haben.

Endpunkt erstellen

Schritte

1. Um einen Load Balancer-Endpunkt zu erstellen, wählen Sie **Endpunkt erstellen**.
2. Füllen Sie für den Schritt **Endpunktdetails eingeben** die folgenden Felder aus.

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt.
Hafen	Der StorageGRID -Port, den Sie für den Lastenausgleich verwenden möchten. Der Standardwert dieses Felds für den ersten Endpunkt, den Sie erstellen, ist 10433. Sie können jedoch jeden beliebigen nicht verwendeten externen Port eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Knoten konfiguriert, da diese Ports auf Admin-Knoten reserviert sind. **Hinweis:** Von anderen Grid-Diensten verwendete Ports sind nicht zulässig. Siehe die"Netzwerkportreferenz" .
Client-Typ	Muss **S3** sein.
Netzwerkprotokoll	Wählen Sie **HTTPS**. **Hinweis**: Die Kommunikation mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen.

3. Geben Sie im Schritt **Bindungsmodus auswählen** den Bindungsmodus an. Der Bindungsmodus steuert, wie auf den Endpunkt über eine beliebige IP-Adresse oder über bestimmte IP-Adressen und Netzwerkschnittstellen zugegriffen wird.

Modus	Beschreibung
Global (Standard)	Clients können über die IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, 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** (Standard), es sei denn, Sie müssen die Erreichbarkeit dieses Endpunkts einschränken.
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder den entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die von Ihnen für die Endpunkte ausgewählten HA-Gruppen nicht überschneiden.

Modus	Beschreibung
Knotenschnittstellen	Clients müssen die IP-Adressen (oder entsprechenden FQDNs) ausgewählter Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Knotentyp	Je nach ausgewähltem 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.

4. Wählen Sie für den Schritt „Mandantenzugriff“ eine der folgenden Optionen aus:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen.
Ausgewählte Mieter blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht verwenden, um auf ihre Buckets zuzugreifen. Alle anderen Mandanten können diesen Endpunkt verwenden.

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

Feld	Beschreibung
Zertifikat hochladen (empfohlen)	Verwenden Sie diese Option, um ein von einer Zertifizierungsstelle signiertes Serverzertifikat, einen privaten Zertifikatsschlüssel und ein optionales CA-Paket hochzuladen.
Zertifikat generieren	Verwenden Sie diese Option, um ein selbstsigniertes Zertifikat zu generieren. Sehen"Konfigurieren von Load Balancer-Endpunkten" für Einzelheiten zu den einzugebenden Informationen.
StorageGRID S3-Zertifikat verwenden	Verwenden Sie diese Option nur, wenn Sie bereits eine benutzerdefinierte Version des globalen StorageGRID -Zertifikats hochgeladen oder generiert haben. Sehen"Konfigurieren von S3-API-Zertifikaten" für Details.

6. Wählen Sie **Fertig**, um zum S3-Setup-Assistenten zurückzukehren.
7. Wählen Sie **Weiter**, um zum Schritt „Mandant und Bucket“ zu gelangen.

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

Vorhandenen Load Balancer-Endpunkt verwenden

Schritte

1. Um einen vorhandenen Endpunkt zu verwenden, wählen Sie seinen Namen aus **Wählen Sie einen Load Balancer-Endpunkt** aus.
2. Wählen Sie **Weiter**, um zum Schritt „Mandant und Bucket“ zu gelangen.

Externen Load Balancer verwenden

Schritte

1. Um einen externen Lastenausgleich zu verwenden, füllen Sie die folgenden Felder aus.

Feld	Beschreibung
FQDN	Der vollqualifizierte Domänenname (FQDN) des externen Load Balancers.
Hafen	Die Portnummer, die die S3-Anwendung zum Herstellen einer Verbindung mit dem externen Load Balancer verwendet.
Zertifikat	Kopieren Sie das Serverzertifikat für den externen Load Balancer und fügen Sie es in dieses Feld ein.

2. Wählen Sie **Weiter**, um zum Schritt „Mandant und Bucket“ zu gelangen.

Schritt 3 von 6: Mandanten und Bucket erstellen

Ein Mandant ist eine Entität, die S3-Anwendungen zum Speichern und Abrufen von Objekten in StorageGRID verwenden kann. Jeder Mandant verfügt über eigene Benutzer, Zugriffsschlüssel, Buckets, Objekte und einen bestimmten Satz an Funktionen.

Ein Bucket ist ein Container zum Speichern der Objekte und Objektmetadaten eines Mandanten. Obwohl Mandanten viele Buckets haben können, hilft Ihnen der Assistent dabei, auf schnellste und einfachste Weise einen Mandanten und einen Bucket zu erstellen. Wenn Sie später Buckets hinzufügen oder Optionen festlegen müssen, können Sie den Tenant Manager verwenden.

Einzelheiten zu dieser Aufgabe finden Sie unter"Mieterkonto erstellen" Und"S3-Bucket erstellen" .

Schritte

1. Geben Sie einen Namen für das Mandantenkonto ein.

   Mandantennamen müssen nicht eindeutig sein. Beim Anlegen des Mandantenkontos erhält dieses eine eindeutige, numerische Konto-ID.

2. Definieren Sie den Root-Zugriff für das Mandantenkonto, je nachdem, ob Ihr StorageGRID -System"Identitätsföderation" ,"Einmaliges Anmelden (SSO)" oder beides.

Option	Tun Sie dies
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das bei der Anmeldung beim Mandanten als lokaler Root-Benutzer verwendet werden soll.

Option	Tun Sie dies
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine bestehende Verbundgruppe aus, die"Root-Zugriffsberechtigung" für den Mieter. b. Geben Sie optional das Kennwort an, das bei der Anmeldung beim Mandanten als lokaler Root-Benutzer verwendet werden soll.
Wenn sowohl die Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine bestehende Verbundgruppe aus, die"Root-Zugriffsberechtigung" für den Mieter. Es können sich keine lokalen Benutzer anmelden.

3. Wenn der Assistent die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den Root-Benutzer erstellen soll, wählen Sie **S3-Zugriffsschlüssel für Root-Benutzer automatisch erstellen**.

   Wählen Sie diese Option, wenn der einzige Benutzer für den Mandanten der Root-Benutzer sein soll. Wenn andere Benutzer diesen Mandanten verwenden,"Verwenden Sie den Tenant Manager" um Schlüssel und Berechtigungen zu konfigurieren.

4. Wenn Sie jetzt einen Bucket für diesen Mandanten erstellen möchten, wählen Sie **Bucket für diesen Mandanten erstellen**.

   Wenn S3 Object Lock für das Raster aktiviert ist, ist S3 Object Lock für den in diesem Schritt erstellten Bucket nicht aktiviert. Wenn Sie für diese S3-Anwendung einen S3 Object Lock-Bucket verwenden müssen, wählen Sie jetzt nicht die Option zum Erstellen eines Buckets aus. Verwenden Sie stattdessen den Tenant Manager, um"Erstellen Sie den Bucket" später.

   a. Geben Sie den Namen des Buckets ein, den die S3-Anwendung verwenden wird. Beispiel: `s3-bucket` .

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

   b. Wählen Sie die **Region** für diesen Bucket aus.

      Verwenden Sie die Standardregion(`us-east-1`), es sei denn, Sie möchten in Zukunft ILM verwenden, um Objekte basierend auf der Region des Buckets zu filtern.

5. Wählen Sie **Erstellen und fortfahren**.

Schritt 4 von 6: Daten herunterladen

Im Schritt „Daten herunterladen“ können Sie eine oder zwei Dateien herunterladen, um die Details Ihrer gerade konfigurierten Daten zu speichern.

Schritte

1. Wenn Sie **S3-Zugriffsschlüssel für Root-Benutzer automatisch erstellen** ausgewählt haben, führen Sie einen oder beide der folgenden Schritte aus:
   - Wählen Sie **Zugriffsschlüssel herunterladen**, um einen `.csv` Datei mit dem Mandantenkontonamen, der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel.
   - Wählen Sie das Kopiersymbol ( ), um die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel

in die Zwischenablage zu kopieren.

2. Wählen Sie **Konfigurationswerte herunterladen**, um eine `.txt` Datei mit den Einstellungen für den Load Balancer-Endpunkt, den Mandanten, den Bucket und den Root-Benutzer.
3. Speichern Sie diese Informationen an einem sicheren Ort.

> Schließen Sie diese Seite erst, wenn Sie beide Zugriffsschlüssel kopiert haben. Die Schlüssel sind nicht mehr verfügbar, nachdem Sie diese Seite geschlossen haben. Stellen Sie sicher, dass Sie diese Informationen an einem sicheren Ort speichern, da sie zum Abrufen von Daten aus Ihrem StorageGRID System verwendet werden können.

4. Aktivieren Sie bei entsprechender Aufforderung das Kontrollkästchen, um zu bestätigen, dass Sie die Schlüssel heruntergeladen oder kopiert haben.
5. Wählen Sie **Weiter** aus, um zum Schritt „ILM-Regel und -Richtlinie“ zu gelangen.

Schritt 5 von 6: ILM-Regel und ILM-Richtlinie für S3 überprüfen

Regeln für das Information Lifecycle Management (ILM) steuern die Platzierung, Dauer und das Aufnahmeverhalten aller Objekte in Ihrem StorageGRID System. Die in StorageGRID enthaltene ILM-Richtlinie erstellt zwei replizierte Kopien aller Objekte. Diese Richtlinie bleibt so lange in Kraft, bis Sie mindestens eine neue Richtlinie aktivieren.

Schritte

1. Überprüfen Sie die auf der Seite bereitgestellten Informationen.
2. Wenn Sie spezifische Anweisungen für die Objekte hinzufügen möchten, die zum neuen Mandanten oder Bucket gehören, erstellen Sie eine neue Regel und eine neue Richtlinie. Sehen"ILM-Regel erstellen" Und"Verwenden von ILM-Richtlinien" .
3. Wählen Sie **Ich habe diese Schritte überprüft und verstehe, was ich tun muss**.
4. Aktivieren Sie das Kontrollkästchen, um anzugeben, dass Sie wissen, was als Nächstes zu tun ist.
5. Wählen Sie **Weiter**, um zur **Zusammenfassung** zu gelangen.

Schritt 6 von 6: Zusammenfassung der Überprüfung

Schritte

1. Lesen Sie die Zusammenfassung.
2. Notieren Sie sich die Details in den nächsten Schritten, in denen die zusätzliche Konfiguration beschrieben wird, die möglicherweise erforderlich ist, bevor Sie eine Verbindung mit dem S3-Client herstellen. Wenn Sie beispielsweise „Als Root Sign in “ auswählen, gelangen Sie zum Mandanten-Manager, wo Sie Mandantenbenutzer hinzufügen, zusätzliche Buckets erstellen und Bucket-Einstellungen aktualisieren können.
3. Wählen Sie **Fertig**.
4. Konfigurieren Sie die Anwendung mithilfe der Datei, die Sie von StorageGRID heruntergeladen haben, oder der Werte, die Sie manuell erhalten haben.

Verwalten von HA-Gruppen

Was sind Hochverfügbarkeitsgruppen (HA)?

Hochverfügbarkeitsgruppen (HA) bieten hochverfügbare Datenverbindungen für S3-Clients und hochverfügbare Verbindungen zum Grid Manager und zum Tenant Manager.

Sie können die Netzwerkschnittstellen mehrerer Admin- und Gateway-Knoten in einer Hochverfügbarkeitsgruppe (HA) zusammenfassen. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle die Arbeitslast bewältigen.

Jede HA-Gruppe bietet Zugriff auf die gemeinsam genutzten Dienste auf den ausgewählten Knoten.

- HA-Gruppen, die Gateway-Knoten, Admin-Knoten oder beides umfassen, bieten hochverfügbare Datenverbindungen für S3-Clients.
- HA-Gruppen, die nur Admin-Knoten enthalten, bieten hochverfügbare Verbindungen zum Grid Manager und zum Tenant Manager.
- Eine HA-Gruppe, die nur Service-Appliances und VMware-basierte Softwareknoten umfasst, kann hochverfügbare Verbindungen bereitstellen für"S3-Mandanten, die S3 Select verwenden" . HA-Gruppen werden bei der Verwendung von S3 Select empfohlen, sind aber nicht erforderlich.

Wie erstellt man eine HA-Gruppe?

1. Sie wählen eine Netzwerkschnittstelle für einen oder mehrere Admin-Knoten oder Gateway-Knoten aus. Sie können eine Grid-Netzwerkschnittstelle (eth0), eine Client-Netzwerkschnittstelle (eth2), eine VLAN-Schnittstelle oder eine Zugriffsschnittstelle verwenden, die Sie dem Knoten hinzugefügt haben.

   > ⓘ Sie können einer HA-Gruppe keine Schnittstelle hinzufügen, wenn diese über eine per DHCP zugewiesene IP-Adresse verfügt.

2. Sie geben eine Schnittstelle als primäre Schnittstelle an. Die primäre Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.
3. Sie bestimmen die Prioritätsreihenfolge für alle Backup-Schnittstellen.
4. Sie weisen der Gruppe eine bis zehn virtuelle IP-Adressen (VIP) zu. Clientanwendungen können jede dieser VIP-Adressen verwenden, um eine Verbindung mit StorageGRID herzustellen.

Anweisungen hierzu finden Sie unter"Konfigurieren von Hochverfügbarkeitsgruppen" .

Was ist die aktive Schnittstelle?

Während des normalen Betriebs werden alle VIP-Adressen für die HA-Gruppe der primären Schnittstelle hinzugefügt, die die erste Schnittstelle in der Prioritätsreihenfolge ist. Solange die primäre Schnittstelle verfügbar bleibt, wird sie verwendet, wenn Clients eine Verbindung mit einer beliebigen VIP-Adresse für die Gruppe herstellen. Das heißt, während des normalen Betriebs ist die primäre Schnittstelle die „aktive“ Schnittstelle für die Gruppe.

Ebenso fungieren während des Normalbetriebs alle Schnittstellen mit niedrigerer Priorität für die HA-Gruppe als „Backup“-Schnittstellen. Diese Backup-Schnittstellen werden nicht verwendet, es sei denn, die primäre (derzeit aktive) Schnittstelle ist nicht mehr verfügbar.

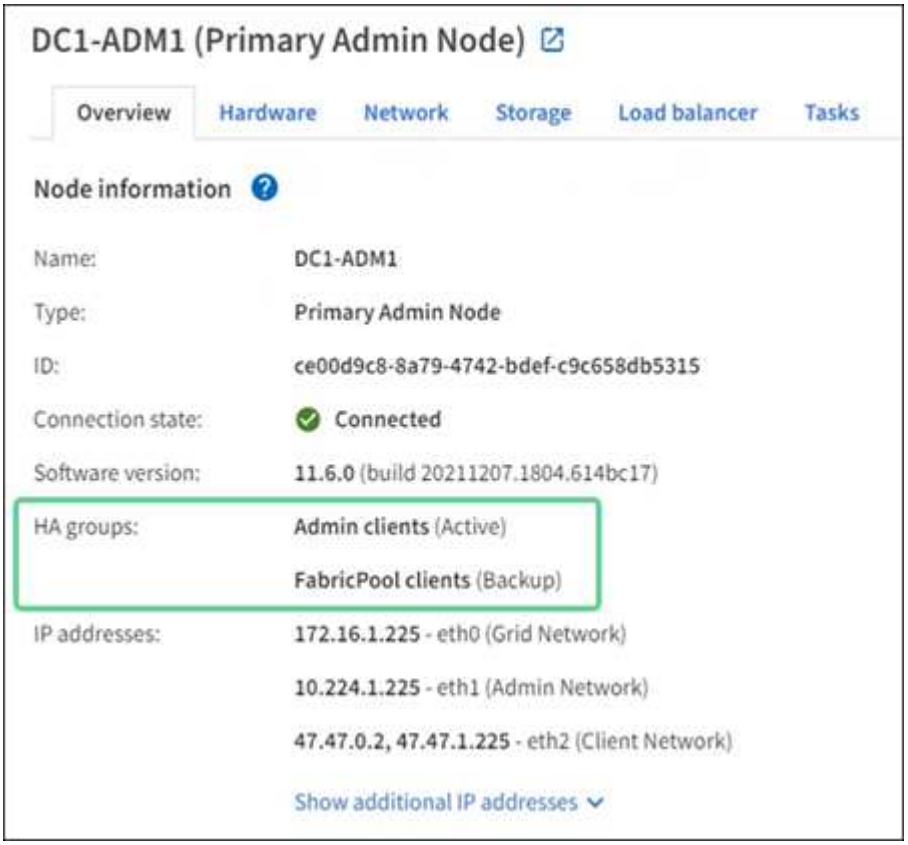
Den aktuellen HA-Gruppenstatus eines Knotens anzeigen

Um zu sehen, ob ein Knoten einer HA-Gruppe zugewiesen ist, und um seinen aktuellen Status zu bestimmen, wählen Sie **NODES** > ***node***.

Wenn die Registerkarte **Übersicht** einen Eintrag für **HA-Gruppen** enthält, wird der Knoten den aufgeführten HA-Gruppen zugewiesen. Der Wert nach dem Gruppennamen ist der aktuelle Status des Knotens in der HA-Gruppe:

- **Aktiv**: Die HA-Gruppe wird derzeit auf diesem Knoten gehostet.
- **Backup**: Die HA-Gruppe verwendet diesen Knoten derzeit nicht. Dies ist eine Backup-Schnittstelle.
- **Gestoppt**: Die HA-Gruppe kann auf diesem Knoten nicht gehostet werden, da der Dienst „High Availability“ (Keepalived) manuell gestoppt wurde.
- **Fehler**: Die HA-Gruppe kann aus einem oder mehreren der folgenden Gründe nicht auf diesem Knoten gehostet werden:
  - Der Load Balancer-Dienst (nginx-gw) wird auf dem Knoten nicht ausgeführt.
  - Die eth0- oder VIP-Schnittstelle des Knotens ist ausgefallen.
  - Der Knoten ist ausgefallen.

In diesem Beispiel wurde der primäre Admin-Knoten zu zwei HA-Gruppen hinzugefügt. Dieser Knoten ist derzeit die aktive Schnittstelle für die Gruppe der Admin-Clients und eine Backup-Schnittstelle für die Gruppe der FabricPool -Clients.



Was passiert, wenn die aktive Schnittstelle ausfällt?

Die Schnittstelle, die derzeit die VIP-Adressen hostet, ist die aktive Schnittstelle. Wenn die HA-Gruppe mehr als eine Schnittstelle umfasst und die aktive Schnittstelle ausfällt, werden die VIP-Adressen in der Prioritätsreihenfolge an die erste verfügbare Backup-Schnittstelle verschoben. Wenn diese Schnittstelle ausfällt, werden die VIP-Adressen zur nächsten verfügbaren Backup-Schnittstelle verschoben und so weiter.

Ein Failover kann aus folgenden Gründen ausgelöst werden:

- Der Knoten, auf dem die Schnittstelle konfiguriert ist, fällt aus.
- Der Knoten, auf dem die Schnittstelle konfiguriert ist, verliert für mindestens 2 Minuten die Verbindung zu allen anderen Knoten.
- Die aktive Schnittstelle fällt aus.
- Der Load Balancer-Dienst wird gestoppt.
- Der Hochverfügbarkeitsdienst wird gestoppt.

> Das Failover wird möglicherweise nicht durch Netzwerkfehler außerhalb des Knotens ausgelöst, der die aktive Schnittstelle hostet. Ebenso wird ein Failover nicht durch die Dienste für den Grid Manager oder den Tenant Manager ausgelöst.

Der Failover-Prozess dauert im Allgemeinen nur wenige Sekunden und ist schnell genug, sodass Client-Anwendungen nur geringe Auswirkungen erfahren und sich auf normale Wiederholungsverhalten verlassen können, um den Betrieb fortzusetzen.

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

Wie werden HA-Gruppen verwendet?

Sie können Hochverfügbarkeitsgruppen (HA) verwenden, um hochverfügbare Verbindungen zu StorageGRID für Objektdaten und zur administrativen Verwendung bereitzustellen.

- Eine HA-Gruppe kann hochverfügbare administrative Verbindungen zum Grid Manager oder Tenant Manager bereitstellen.
- Eine HA-Gruppe kann hochverfügbare Datenverbindungen für S3-Clients bereitstellen.
- Eine HA-Gruppe, die nur eine Schnittstelle enthält, ermöglicht Ihnen die Bereitstellung vieler VIP-Adressen und die explizite Festlegung von IPv6-Adressen.

Eine HA-Gruppe kann nur dann eine hohe Verfügbarkeit bieten, wenn alle in der Gruppe enthaltenen Knoten dieselben Dienste bereitstellen. Wenn Sie eine HA-Gruppe erstellen, fügen Sie Schnittstellen von den Knotentypen hinzu, die die von Ihnen benötigten Dienste bereitstellen.

- **Admin-Knoten**: Schließen Sie den Load Balancer-Dienst ein und ermöglichen Sie den Zugriff auf den Grid Manager oder den Tenant Manager.
- **Gateway-Knoten**: Schließen Sie den Load Balancer-Dienst ein.

Zweck der HA-Gruppe	Knoten dieses Typs zur HA-Gruppe hinzufügen
Zugriff auf Grid Manager	• Primärer Admin-Knoten (**Primär**) • Nicht-primäre Admin-Knoten **Hinweis:** Der primäre Admin-Knoten muss die primäre Schnittstelle sein. Einige Wartungsvorgänge können nur vom primären Admin-Knoten aus durchgeführt werden.

Zweck der HA-Gruppe	Knoten dieses Typs zur HA-Gruppe hinzufügen
Zugriff nur auf den Mandantenmanager	• Primäre oder nicht-primäre Admin-Knoten
S3-Clientzugriff – Load Balancer-Dienst	• Admin-Knoten • Gateway-Knoten
S3-Client-Zugriff für"S3 Auswählen"	• Servicegeräte • VMware-basierte Softwareknoten **Hinweis**: HA-Gruppen werden bei der Verwendung von S3 Select empfohlen, sind aber nicht erforderlich.

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

Wenn ein Grid Manager- oder Tenant Manager-Dienst ausfällt, wird kein HA-Gruppen-Failover ausgelöst.

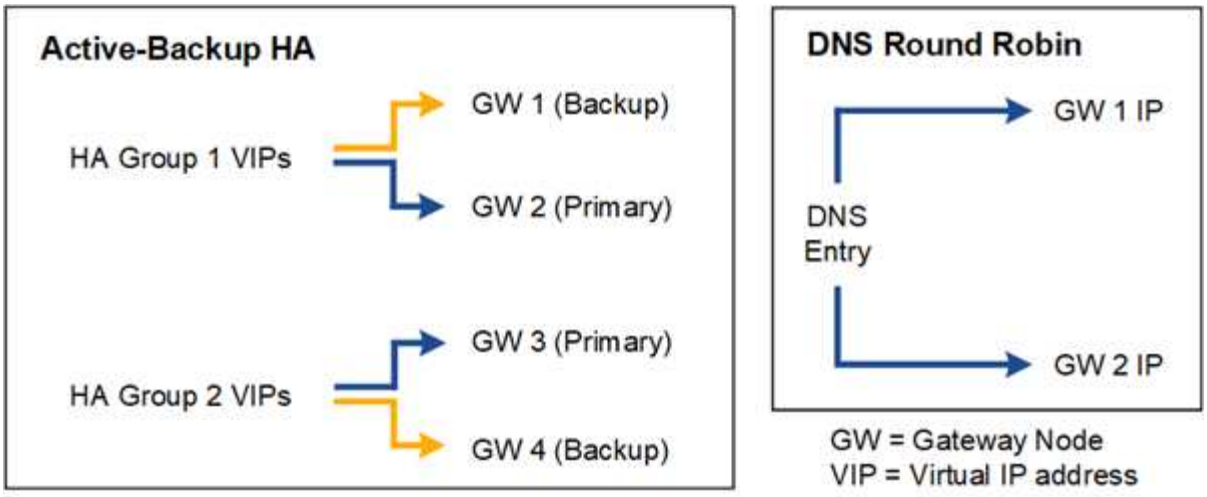
Wenn Sie beim Failover beim Grid Manager oder Tenant Manager angemeldet sind, werden Sie abgemeldet und müssen sich erneut anmelden, um Ihre Aufgabe fortzusetzen.

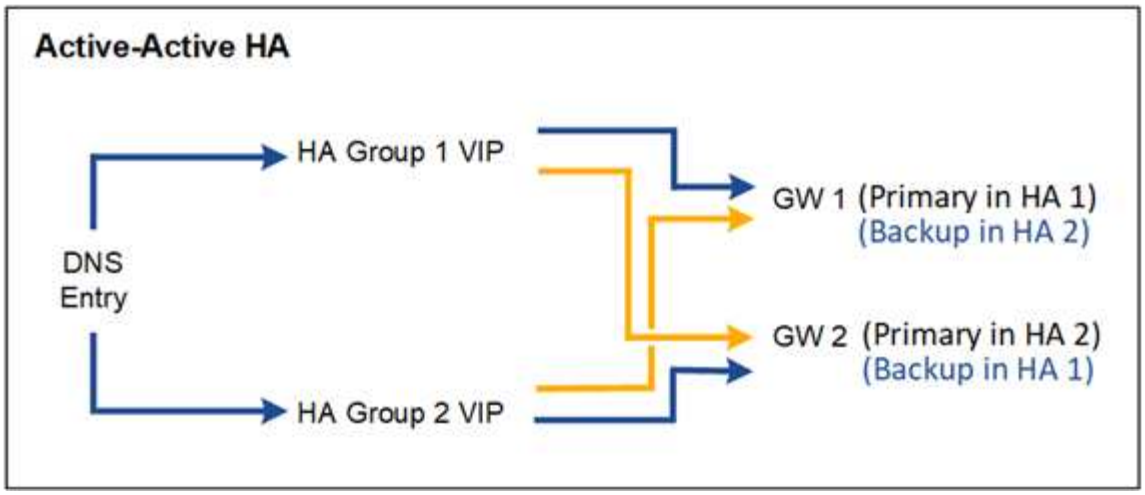
Einige Wartungsverfahren können nicht durchgeführt werden, wenn der primäre Admin-Knoten nicht verfügbar ist. Während des Failovers können Sie den Grid Manager verwenden, um Ihr StorageGRID System zu überwachen.

Konfigurationsoptionen für HA-Gruppen

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

In den Diagrammen kennzeichnet Blau die primäre Schnittstelle in der HA-Gruppe und Gelb die Backup-Schnittstelle in der HA-Gruppe.





Die Tabelle fasst die Vorteile jeder im Diagramm gezeigten HA-Konfiguration zusammen.

Konfiguration	Vorteile	Nachteile
Active-Backup HA	• Verwaltet von StorageGRID ohne externe Abhängigkeiten. • Schnelles Failover.	• In einer HA-Gruppe ist nur ein Knoten aktiv. Mindestens ein Knoten pro HA-Gruppe ist im Leerlauf.
DNS-Round-Robin	• Erhöhter Gesamtdurchsatz. • Keine untätigen Hosts.	• Langsames Failover, das vom Clientverhalten abhängen kann. • Erfordert die Konfiguration der Hardware außerhalb von StorageGRID. • Benötigt einen vom Kunden durchgeführten Gesundheitscheck.

Konfiguration	Vorteile	Nachteile
Aktiv-Aktiv-HA	• Der Datenverkehr wird auf mehrere HA-Gruppen verteilt. • Hoher Gesamtdurchsatz, der mit der Anzahl der HA-Gruppen skaliert. • Schnelles Failover.	• Komplexer zu konfigurieren. • Erfordert die Konfiguration der Hardware außerhalb von StorageGRID. • Benötigt einen vom Kunden durchgeführten Gesundheitscheck.

Konfigurieren von Hochverfügbarkeitsgruppen

Sie können Hochverfügbarkeitsgruppen (HA) konfigurieren, um einen hochverfügbaren Zugriff auf die Dienste auf Admin-Knoten oder Gateway-Knoten bereitzustellen.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .
- Wenn Sie eine VLAN-Schnittstelle in einer HA-Gruppe verwenden möchten, haben Sie die VLAN-Schnittstelle erstellt. Sehen "Konfigurieren von VLAN-Schnittstellen" .
- Wenn Sie eine Zugriffsschnittstelle für einen Knoten in einer HA-Gruppe verwenden möchten, haben Sie die Schnittstelle erstellt:
  - **Red Hat Enterprise Linux (vor der Installation des Knotens)**:"Erstellen Sie Knotenkonfigurationsdateien"
  - **Ubuntu oder Debian (vor der Installation des Knotens)**:"Erstellen Sie Knotenkonfigurationsdateien"
  - **Linux (nach der Installation des Knotens)**:"Linux: Trunk oder Zugriffsschnittstellen zu einem Knoten hinzufügen"
  - **VMware (nach der Installation des Knotens)**:"VMware: Trunk- oder Zugriffsschnittstellen zu einem Knoten hinzufügen"

Erstellen einer Hochverfügbarkeitsgruppe

Wenn Sie eine Hochverfügbarkeitsgruppe erstellen, wählen Sie eine oder mehrere Schnittstellen aus und organisieren sie nach Priorität. Anschließend weisen Sie der Gruppe eine oder mehrere VIP-Adressen zu.

Eine Schnittstelle muss für einen Gateway-Knoten oder einen Admin-Knoten sein, um in eine HA-Gruppe aufgenommen zu werden. Eine HA-Gruppe kann für jeden Knoten nur eine Schnittstelle verwenden. In anderen HA-Gruppen können jedoch andere Schnittstellen für denselben Knoten verwendet werden.

Zugriff auf den Assistenten

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Hochverfügbarkeitsgruppen**.
2. Wählen Sie **Erstellen**.

Geben Sie Details für die HA-Gruppe ein

Schritte

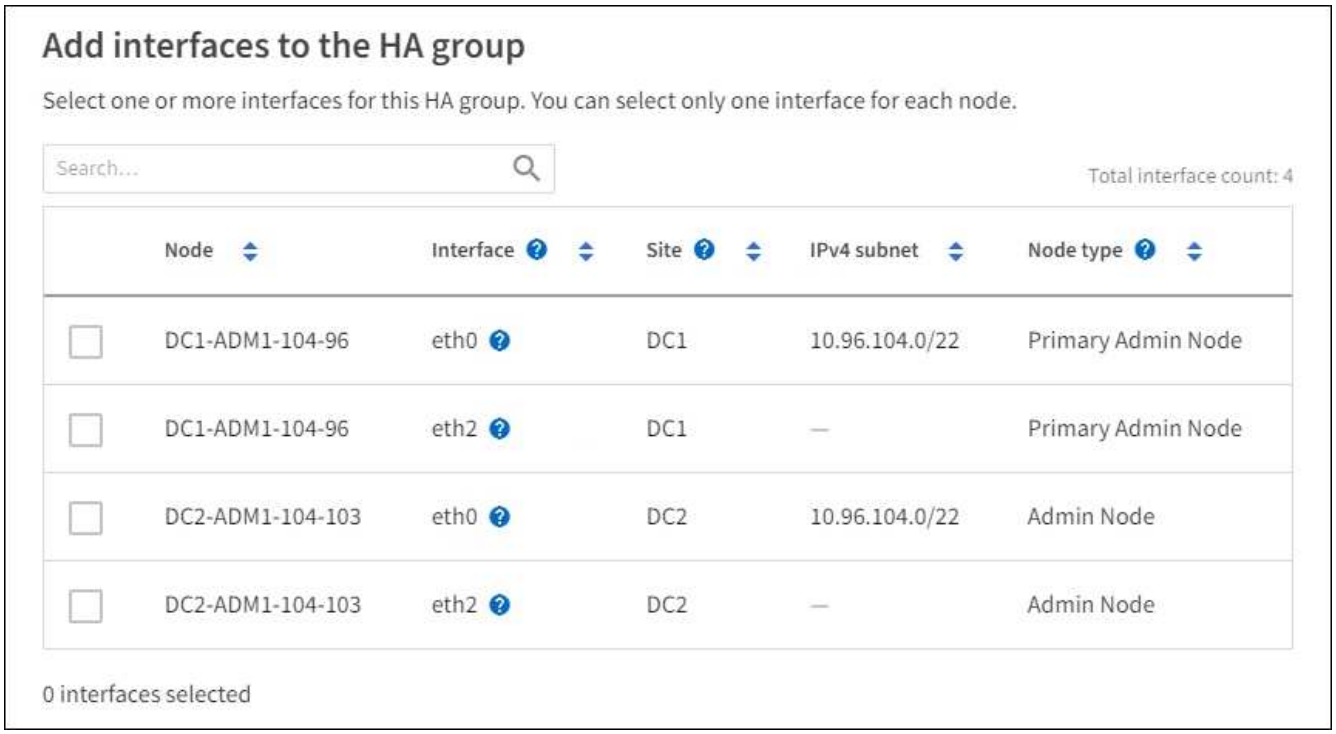
1. Geben Sie einen eindeutigen Namen für die HA-Gruppe an.
2. Geben Sie optional eine Beschreibung für die HA-Gruppe ein.
3. Wählen Sie **Weiter**.

Schnittstellen zur HA-Gruppe hinzufügen

Schritte

1. Wählen Sie eine oder mehrere Schnittstellen aus, die dieser HA-Gruppe hinzugefügt werden sollen.

   Nutzen Sie die Spaltenüberschriften zum Sortieren der Zeilen oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.

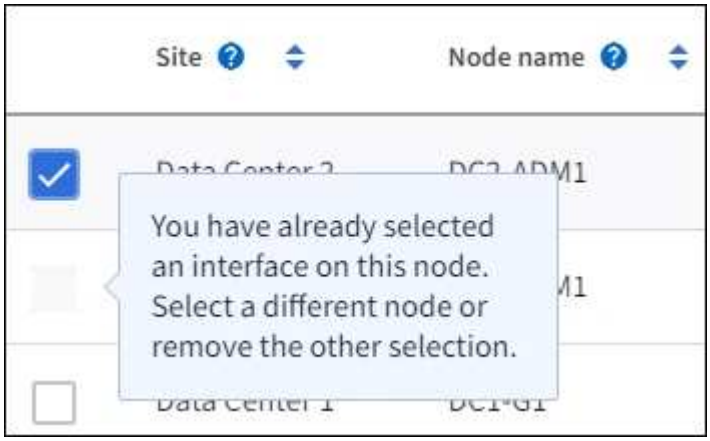


> Warten Sie nach dem Erstellen einer VLAN-Schnittstelle bis zu 5 Minuten, bis die neue Schnittstelle in der Tabelle angezeigt wird.

Richtlinien zur Auswahl von Schnittstellen

- Sie müssen mindestens eine Schnittstelle auswählen.
- Sie können für einen Knoten nur eine Schnittstelle auswählen.
- Wenn die HA-Gruppe zum HA-Schutz von Admin-Node-Diensten dient, zu denen der Grid Manager und der Tenant Manager gehören, wählen Sie nur Schnittstellen auf Admin-Nodes aus.
- Wenn die HA-Gruppe dem HA-Schutz des S3-Client-Datenverkehrs dient, wählen Sie Schnittstellen auf Admin-Knoten, Gateway-Knoten oder beiden aus.
- Wenn Sie Schnittstellen auf verschiedenen Knotentypen auswählen, wird ein Hinweis angezeigt. Bitte beachten Sie, dass bei einem Failover die vom zuvor aktiven Knoten bereitgestellten Dienste auf dem neuen aktiven Knoten möglicherweise nicht verfügbar sind. Beispielsweise kann ein Backup-Gateway-Knoten keinen HA-Schutz für Admin-Knotendienste bieten. Ebenso kann ein Backup-Admin-Knoten nicht alle Wartungsverfahren durchführen, die der primäre Admin-Knoten bereitstellen kann.
- Wenn Sie keine Schnittstelle auswählen können, ist das entsprechende Kontrollkästchen deaktiviert.

Der Tooltip bietet weitere Informationen.



- Sie können keine Schnittstelle auswählen, wenn ihr Subnetzwert oder Gateway mit einer anderen ausgewählten Schnittstelle in Konflikt steht.
- Sie können eine konfigurierte Schnittstelle nicht auswählen, wenn sie keine statische IP-Adresse hat.

2. Wählen Sie **Weiter**.

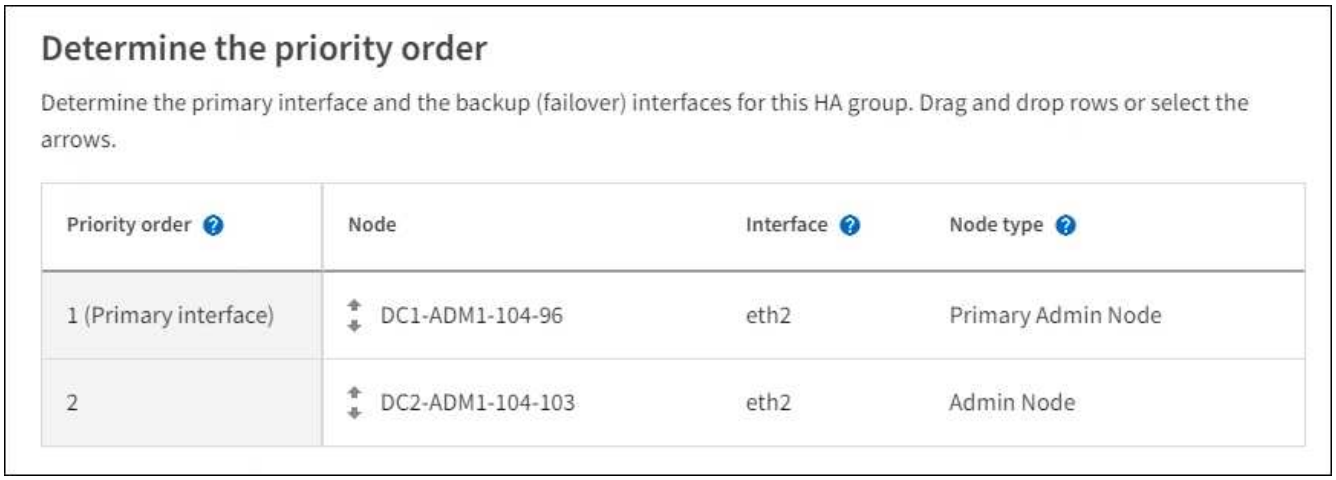
Bestimmen Sie die Prioritätsreihenfolge

Wenn die HA-Gruppe mehr als eine Schnittstelle umfasst, können Sie bestimmen, welche die primäre Schnittstelle und welche die Backup-Schnittstellen (Failover) sind. Wenn die primäre Schnittstelle ausfällt, werden die VIP-Adressen an die verfügbare Schnittstelle mit der höchsten Priorität weitergeleitet. Wenn diese Schnittstelle ausfällt, werden die VIP-Adressen zur nächsten verfügbaren Schnittstelle mit der höchsten Priorität verschoben und so weiter.

Schritte

1. Ziehen Sie Zeilen in der Spalte **Prioritätsreihenfolge**, um die primäre Schnittstelle und alle Backup-Schnittstellen zu bestimmen.

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



Wenn die HA-Gruppe Zugriff auf den Grid Manager bietet, müssen Sie eine Schnittstelle auf dem primären Admin-Knoten als primäre Schnittstelle auswählen. Einige Wartungsvorgänge können nur vom primären Admin-Knoten aus durchgeführt werden.

2. Wählen Sie **Weiter**.

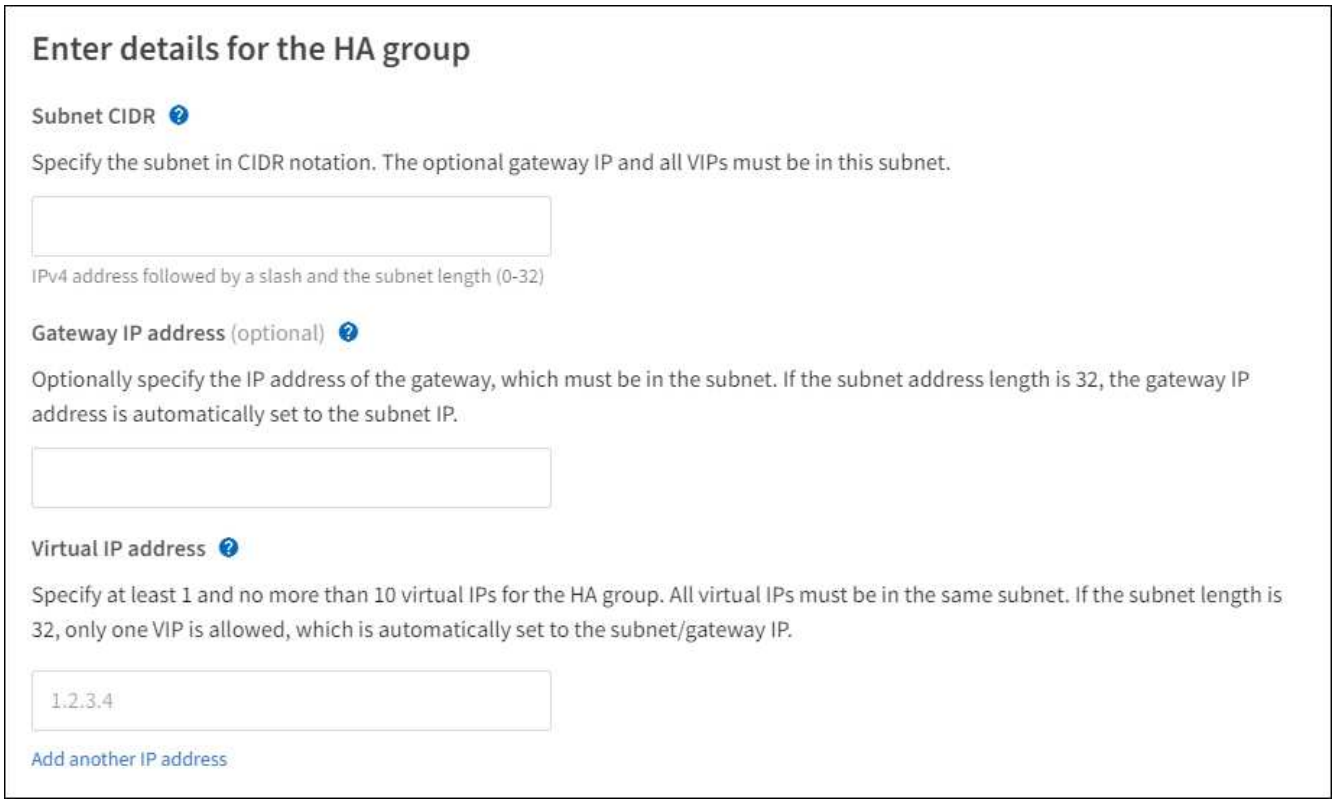
IP-Adressen eingeben

Schritte

1. Geben Sie im Feld **Subnetz-CIDR** das VIP-Subnetz in CIDR-Notation an – eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetzlänge (0–32).

   Für die Netzwerkadresse dürfen keine Hostbits gesetzt sein. Beispiel: `192.16.0.0/22`.

   > Wenn Sie ein 32-Bit-Präfix verwenden, dient die VIP-Netzwerkadresse auch als Gateway-Adresse und VIP-Adresse.



2. Wenn S3-Verwaltungs- oder Mandantenclients von einem anderen Subnetz aus auf diese VIP-Adressen zugreifen, geben Sie optional die **Gateway-IP-Adresse** ein. Die Gateway-Adresse muss innerhalb des VIP-Subnetzes liegen.

   Client- und Administratorbenutzer verwenden dieses Gateway, um auf die virtuellen IP-Adressen zuzugreifen.

3. Geben Sie mindestens eine und höchstens zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden und alle müssen gleichzeitig auf der aktiven Schnittstelle aktiv sein.

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

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

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

Nächste Schritte

Wenn Sie diese HA-Gruppe zum Lastenausgleich verwenden möchten, erstellen Sie einen Lastenausgleichsendpunkt, um den Port und das Netzwerkprotokoll zu bestimmen und alle erforderlichen Zertifikate anzuhängen. Sehen "Konfigurieren von Load Balancer-Endpunkten" .

Bearbeiten einer Hochverfügbarkeitsgruppe

Sie können eine Hochverfügbarkeitsgruppe (HA) bearbeiten, um ihren Namen und ihre Beschreibung zu ändern, Schnittstellen hinzuzufügen oder zu entfernen, die Prioritätsreihenfolge zu ändern oder virtuelle IP-Adressen hinzuzufügen oder zu aktualisieren.

Beispielsweise müssen Sie möglicherweise eine HA-Gruppe bearbeiten, wenn Sie den Knoten entfernen möchten, der einer ausgewählten Schnittstelle in einem Site- oder Knoten-Außerbetriebnahmeverfahren zugeordnet ist.

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Hochverfügbarkeitsgruppen**.

   Auf der Seite „Hochverfügbarkeitsgruppen“ werden alle vorhandenen HA-Gruppen angezeigt.

2. Aktivieren Sie das Kontrollkästchen für die HA-Gruppe, die Sie bearbeiten möchten.
3. Führen Sie je nachdem, was Sie aktualisieren möchten, einen der folgenden Schritte aus:
   - Wählen Sie **Aktionen** > **Virtuelle IP-Adresse bearbeiten**, um VIP-Adressen hinzuzufügen oder zu entfernen.
   - Wählen Sie **Aktionen** > **HA-Gruppe bearbeiten**, um den Namen oder die Beschreibung der Gruppe zu aktualisieren, Schnittstellen hinzuzufügen oder zu entfernen, die Prioritätsreihenfolge zu ändern oder VIP-Adressen hinzuzufügen oder zu entfernen.
4. Wenn Sie **Virtuelle IP-Adresse bearbeiten** ausgewählt haben:
   a. Aktualisieren Sie die virtuellen IP-Adressen für die HA-Gruppe.
   b. Wählen Sie **Speichern**.
   c. Wählen Sie **Fertig**.
5. Wenn Sie **HA-Gruppe bearbeiten** ausgewählt haben:
   a. Aktualisieren Sie optional den Namen oder die Beschreibung der Gruppe.
   b. Aktivieren oder deaktivieren Sie optional die Kontrollkästchen, um Schnittstellen hinzuzufügen oder zu entfernen.

      Wenn die HA-Gruppe Zugriff auf den Grid Manager bietet, müssen Sie eine Schnittstelle auf dem primären Admin-Knoten als primäre Schnittstelle auswählen. Einige Wartungsvorgänge können nur vom primären Admin-Knoten aus durchgeführt werden

   c. Ziehen Sie optional Zeilen, um die Prioritätsreihenfolge der primären Schnittstelle und aller Backup-Schnittstellen für diese HA-Gruppe zu ändern.
   d. Aktualisieren Sie optional die virtuellen IP-Adressen.
   e. Wählen Sie **Speichern** und dann **Fertig**.

Entfernen einer Hochverfügbarkeitsgruppe

Sie können eine oder mehrere Hochverfügbarkeitsgruppen (HA) gleichzeitig entfernen.

> Sie können eine HA-Gruppe nicht entfernen, wenn sie an einen Load Balancer-Endpunkt gebunden ist. Um eine HA-Gruppe zu löschen, müssen Sie sie von allen Load Balancer-Endpunkten entfernen, die sie verwenden.

Um Clientunterbrechungen zu vermeiden, aktualisieren Sie alle betroffenen S3-Clientanwendungen, bevor Sie eine HA-Gruppe entfernen. Aktualisieren Sie jeden Client, um eine Verbindung über eine andere IP-Adresse herzustellen, beispielsweise die virtuelle IP-Adresse einer anderen HA-Gruppe oder die IP-Adresse, die während der Installation für eine Schnittstelle konfiguriert wurde.

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Hochverfügbarkeitsgruppen**.
2. Überprüfen Sie die Spalte **Load Balancer-Endpunkte** für jede HA-Gruppe, die Sie entfernen möchten. Wenn Load Balancer-Endpunkte aufgelistet sind:
   a. Gehen Sie zu **KONFIGURATION** > **Netzwerk** > **Load Balancer-Endpunkte**.
   b. Aktivieren Sie das Kontrollkästchen für den Endpunkt.
   c. Wählen Sie **Aktionen** > **Endpunktbindungsmodus bearbeiten**.
   d. Aktualisieren Sie den Bindungsmodus, um die HA-Gruppe zu entfernen.
   e. Wählen Sie **Änderungen speichern**.
3. Wenn keine Load Balancer-Endpunkte aufgelistet sind, aktivieren Sie das Kontrollkästchen für jede HA-Gruppe, die Sie entfernen möchten.
4. Wählen Sie **Aktionen** > **HA-Gruppe entfernen**.
5. Überprüfen Sie die Nachricht und wählen Sie **HA-Gruppe löschen**, um Ihre Auswahl zu bestätigen.

   Alle von Ihnen ausgewählten HA-Gruppen werden entfernt. Auf der Seite „Hochverfügbarkeitsgruppen“ wird ein grünes Erfolgsbanner angezeigt.

Verwalten des Lastenausgleichs

Überlegungen zum Lastenausgleich

Sie können den Lastenausgleich verwenden, um die Aufnahme- und Abruf-Workloads von S3-Clients zu verarbeiten.

Was ist Lastenausgleich?

Wenn eine Clientanwendung Daten auf einem StorageGRID -System speichert oder abruft, verwendet StorageGRID einen Load Balancer, um die Arbeitslast für Aufnahme und Abruf zu verwalten. Durch Lastenausgleich werden Geschwindigkeit und Verbindungskapazität maximiert, indem die Arbeitslast auf mehrere Speicherknoten verteilt wird.

Der StorageGRID Load Balancer-Dienst ist auf allen Admin-Knoten und allen Gateway-Knoten installiert und bietet Layer 7-Lastausgleich. Es führt die Transport Layer Security (TLS)-Terminierung von Clientanforderungen durch, überprüft die Anforderungen und stellt neue sichere Verbindungen zu den Speicherknoten her.

Der Load Balancer-Dienst auf jedem Knoten arbeitet unabhängig, wenn er Client-Datenverkehr an die Speicherknoten weiterleitet. Durch einen Gewichtungsprozess leitet der Load Balancer-Dienst mehr Anfragen an Speicherknoten mit höherer CPU-Verfügbarkeit weiter.

> Obwohl der StorageGRID Load Balancer-Dienst der empfohlene Lastausgleichsmechanismus ist, möchten Sie möglicherweise stattdessen einen Load Balancer eines Drittanbieters integrieren. Weitere Informationen erhalten Sie von Ihrem NetApp Kundenbetreuer oder unter "TR-4626: StorageGRID Load Balancer von Drittanbietern und globale Load Balancer" .

Wie viele Lastausgleichsknoten benötige ich?

Als allgemeine Best Practice sollte jede Site in Ihrem StorageGRID -System zwei oder mehr Knoten mit dem Load Balancer-Dienst enthalten. Beispielsweise kann eine Site zwei Gateway-Knoten oder sowohl einen Admin-Knoten als auch einen Gateway-Knoten enthalten. Stellen Sie sicher, dass für jeden Lastausgleichsknoten eine angemessene Netzwerk-, Hardware- oder Virtualisierungsinfrastruktur vorhanden ist, unabhängig davon, ob Sie Service-Appliances, Bare-Metal-Knoten oder Knoten auf Basis virtueller Maschinen (VM) verwenden.

Was ist ein Load Balancer-Endpunkt?

Ein Load Balancer-Endpunkt definiert den Port und das Netzwerkprotokoll (HTTPS oder HTTP), die eingehende und ausgehende Client-Anwendungsanforderungen verwenden, um auf die Knoten zuzugreifen, die den Load Balancer-Dienst enthalten. Der Endpunkt definiert auch den Clienttyp (S3), den Bindungsmodus und optional eine Liste zulässiger oder blockierter Mandanten.

Um einen Load Balancer-Endpunkt zu erstellen, wählen Sie entweder **KONFIGURATION** > **Netzwerk** > **Load Balancer-Endpunkte** oder schließen Sie den FabricPool und S3-Setup-Assistenten ab. Anweisungen:

- "Konfigurieren von Load Balancer-Endpunkten"
- "Verwenden Sie den S3-Setup-Assistenten"
- "Verwenden des FabricPool -Setup-Assistenten"

Überlegungen zum Port

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

Von anderen Grid-Diensten verwendete Ports sind nicht zulässig. Siehe die"Netzwerkportreferenz" .

Überlegungen zum Netzwerkprotokoll

In den meisten Fällen sollten die Verbindungen zwischen Clientanwendungen und StorageGRID die Transport Layer Security (TLS)-Verschlüsselung verwenden. Die Verbindung zu StorageGRID ohne TLS-Verschlüsselung wird unterstützt, wird jedoch insbesondere in Produktionsumgebungen nicht empfohlen. Wenn Sie das Netzwerkprotokoll für den StorageGRID Load Balancer-Endpunkt auswählen, sollten Sie **HTTPS** auswählen.

Überlegungen zu Load Balancer-Endpunktzertifikaten

Wenn Sie **HTTPS** als Netzwerkprotokoll für den Load Balancer-Endpunkt auswählen, müssen Sie ein

Sicherheitszertifikat angeben. Sie können beim Erstellen des Load Balancer-Endpunkts eine dieser drei Optionen verwenden:

- **Laden Sie ein signiertes Zertifikat hoch (empfohlen)**. Dieses Zertifikat kann entweder von einer öffentlich vertrauenswürdigen oder einer privaten Zertifizierungsstelle (CA) signiert sein. Die beste Vorgehensweise besteht darin, zur Sicherung der Verbindung ein öffentlich vertrauenswürdiges CA-Serverzertifikat zu verwenden. Im Gegensatz zu generierten Zertifikaten können von einer Zertifizierungsstelle signierte Zertifikate unterbrechungsfrei rotiert werden, wodurch Ablaufprobleme vermieden werden können.

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

  - Die benutzerdefinierte Serverzertifikatsdatei.
  - Die private Schlüsseldatei des benutzerdefinierten Serverzertifikats.
  - Optional ein CA-Bündel der Zertifikate von jeder zwischengeschalteten ausstellenden Zertifizierungsstelle.
- **Erstellen Sie ein selbstsigniertes Zertifikat**.
- **Verwenden Sie das globale StorageGRID S3-Zertifikat**. Sie müssen eine benutzerdefinierte Version dieses Zertifikats hochladen oder generieren, bevor Sie es für den Load Balancer-Endpunkt auswählen können. Sehen "Konfigurieren von S3-API-Zertifikaten" .

Welche Werte benötige ich?

Um das Zertifikat zu erstellen, müssen Sie alle Domänennamen und IP-Adressen kennen, die S3-Clientanwendungen für den Zugriff auf den Endpunkt verwenden.

Der **Subject DN**-Eintrag (Distinguished Name) für das Zertifikat muss den vollqualifizierten Domänennamen enthalten, den die Clientanwendung 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 vollqualifizierten Domänennamen aller Admin-Knoten und Gateway-Knoten darzustellen, auf denen der Load Balancer-Dienst ausgeführt wird. Zum Beispiel, `*.storagegrid.example.com` verwendet das Platzhalterzeichen * zur Darstellung `adm1.storagegrid.example.com` Und `gn1.storagegrid.example.com` .

Wenn Sie S3 Virtual Hosted-Style-Anfragen verwenden möchten, muss das Zertifikat auch einen **Alternative Name**-Eintrag für jeden"S3-Endpunktdomänenname" Sie haben alle konfigurierten Namen, einschließlich aller Platzhalternamen. Beispiel:

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

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

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

Wie verwalte ich ablaufende Zertifikate?

> Wenn das zum Sichern der Verbindung zwischen der S3-Anwendung und StorageGRID verwendete Zertifikat abläuft, verliert die Anwendung möglicherweise vorübergehend den Zugriff auf StorageGRID.

Um Probleme mit dem Ablauf von Zertifikaten zu vermeiden, befolgen Sie diese Best Practices:

- Überwachen Sie sorgfältig alle Warnungen, die vor dem nahenden Ablaufdatum von Zertifikaten warnen, wie etwa die Warnungen „Ablauf des Load Balancer-Endpunktzertifikats“ und „Ablauf des globalen Serverzertifikats für S3-API“.
- Halten Sie die Zertifikatsversionen der StorageGRID und S3-Anwendung immer synchron. Wenn Sie das für einen Load Balancer-Endpunkt verwendete Zertifikat ersetzen oder erneuern, müssen Sie das entsprechende Zertifikat ersetzen oder erneuern, das von der S3-Anwendung verwendet wird.
- Verwenden Sie ein öffentlich signiertes CA-Zertifikat. Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat verwenden, können Sie bald ablaufende Zertifikate unterbrechungsfrei ersetzen.
- Wenn Sie ein selbstsigniertes StorageGRID -Zertifikat generiert haben und dieses Zertifikat bald abläuft, müssen Sie das Zertifikat sowohl in StorageGRID als auch in der S3-Anwendung manuell ersetzen, bevor das vorhandene Zertifikat abläuft.

Überlegungen zum Bindungsmodus

Mit dem Bindungsmodus können Sie steuern, 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 vollqualifizierten Domänennamen (FQDN) verwenden. Clientanwendungen, die eine andere IP-Adresse oder einen anderen FQDN verwenden, können nicht auf den Endpunkt zugreifen.

Sie können einen der folgenden Bindungsmodi angeben:

- **Global** (Standard): Clientanwendungen können über die IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie diese Einstellung, es sei denn, Sie müssen die Erreichbarkeit eines Endpunkts einschränken.
- **Virtuelle IPs von HA-Gruppen**. Clientanwendungen müssen eine virtuelle IP-Adresse (oder den entsprechenden FQDN) einer HA-Gruppe verwenden.
- **Knotenschnittstellen**. Clients müssen die IP-Adressen (oder entsprechenden FQDNs) ausgewählter Knotenschnittstellen verwenden.
- **Knotentyp**. Je nach ausgewähltem 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 zum Mandantenzugriff

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

Sie können diese Funktion verwenden, um eine bessere Sicherheitsisolierung zwischen Mandanten und ihren Endpunkten bereitzustellen. Sie können diese Funktion beispielsweise verwenden, um sicherzustellen, dass streng geheime oder streng geheime Materialien im Besitz eines Mieters für andere Mieter völlig unzugänglich

bleiben.

> Zum Zwecke der Zugriffskontrolle wird der Mandant anhand der in der Client-Anforderung verwendeten Zugriffsschlüssel ermittelt. Wenn im Rahmen der Anforderung keine Zugriffsschlüssel bereitgestellt werden (z. B. bei anonymem Zugriff), wird der Bucket-Eigentümer zur Ermittlung des Mandanten verwendet.

Beispiel für den Mandantenzugriff

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

1. Sie haben wie folgt zwei Load Balancer-Endpunkte erstellt:
   - **Öffentlicher** Endpunkt: Verwendet Port 10443 und ermöglicht allen Mandanten den Zugriff.
   - **Streng geheim**-Endpunkt: Verwendet Port 10444 und ermöglicht nur dem **Streng geheim**-Mandanten Zugriff. Allen anderen Mandanten ist der Zugriff auf diesen Endpunkt untersagt.
2. Der `top-secret.pdf` befindet sich in einem Eimer, der dem **streng geheimen** Mieter gehört.

Um auf die `top-secret.pdf` kann ein Benutzer im Mandanten **Top secret** eine GET-Anfrage an `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 jedoch ein Benutzer eines anderen Mandanten dieselbe Anfrage an dieselbe URL sendet, erhält er sofort die Meldung „Zugriff verweigert“. Der Zugriff wird verweigert, auch wenn die Anmeldeinformationen und die Signatur gültig sind.

CPU-Verfügbarkeit

Der Load Balancer-Dienst auf jedem Admin-Knoten und Gateway-Knoten arbeitet unabhängig, wenn er S3-Verkehr an die Speicherknoten weiterleitet. Durch einen Gewichtungsprozess leitet der Load Balancer-Dienst mehr Anfragen an Speicherknoten 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 Speicherknoten wird ein minimaler Basisgewichtungswert zugewiesen, auch wenn ein Knoten eine Auslastung von 100 % meldet oder seine Auslastung nicht meldet.

In einigen Fällen sind Informationen zur CPU-Verfügbarkeit auf den Standort beschränkt, an dem sich der Load Balancer-Dienst befindet.

Konfigurieren von Load Balancer-Endpunkten

Load Balancer-Endpunkte bestimmen die Ports und Netzwerkprotokolle, die S3-Clients beim Herstellen einer Verbindung mit dem StorageGRID Load Balancer auf Gateway- und Admin-Knoten verwenden können. Sie können auch Endpunkte verwenden, um auf den Grid Manager, den Tenant Manager oder beide zuzugreifen.

> Swift-Details wurden aus dieser Version der Dokumentationssite entfernt. Sehen "Konfigurieren Sie S3- und Swift-Clientverbindungen" .

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .
- Sie haben die"Überlegungen zum Lastenausgleich" .

- Wenn Sie zuvor einen Port neu zugeordnet haben, den Sie für den Load Balancer-Endpunkt verwenden möchten, müssen Sie"die Port-Neuzuordnung wurde entfernt" .
- Sie haben alle Hochverfügbarkeitsgruppen (HA) erstellt, die Sie verwenden möchten. HA-Gruppen werden empfohlen, sind aber nicht erforderlich. Sehen "Verwalten von Hochverfügbarkeitsgruppen" .
- Wenn der Load Balancer-Endpunkt verwendet wird von"S3-Mandanten für S3 Select" , es dürfen nicht die IP-Adressen oder FQDNs von Bare-Metal-Knoten verwendet werden. Für die für S3 Select verwendeten Load Balancer-Endpunkte sind nur Service-Appliances und VMware-basierte Softwareknoten zulässig.
- Sie haben alle VLAN-Schnittstellen konfiguriert, die Sie verwenden möchten. Sehen "Konfigurieren von VLAN-Schnittstellen" .
- Wenn Sie einen HTTPS-Endpunkt erstellen (empfohlen), verfügen Sie über die Informationen für das Serverzertifikat.

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

  - Zum Hochladen eines Zertifikats benötigen Sie das Serverzertifikat, den privaten Zertifikatsschlüssel und optional ein CA-Paket.
  - Zum Generieren eines Zertifikats benötigen Sie alle Domänennamen und IP-Adressen, die S3-Clients für den Zugriff auf den Endpunkt verwenden. Sie müssen auch den Betreff (Distinguished Name) kennen.
  - Wenn Sie das StorageGRID S3-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 wurde. Sehen "Konfigurieren von S3-API-Zertifikaten" .

Erstellen eines Load Balancer-Endpunkts

Jeder S3-Client-Load-Balancer-Endpunkt gibt einen Port, einen Clienttyp (S3) und ein Netzwerkprotokoll (HTTP oder HTTPS) an. Die Endpunkte des Lastenausgleichsmoduls der Verwaltungsschnittstelle geben einen Port, einen Schnittstellentyp und ein nicht vertrauenswürdiges Clientnetzwerk an.

Zugriff auf den Assistenten

Schritte

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

Geben Sie die Endpunktdetails ein

Schritte

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

S3- oder Swift-Client

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt, der in der Tabelle auf der Seite „Load Balancer-Endpunkte“ angezeigt wird.
Hafen	Der StorageGRID -Port, den Sie für den Lastenausgleich verwenden möchten. Der Standardwert dieses Felds für den ersten Endpunkt, den Sie erstellen, ist 10433. 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-Knoten konfiguriert, es sei denn, Sie haben Port 8443 freigegeben. Dann können Sie Port 8443 als S3-Endpunkt verwenden und der Port wird sowohl auf dem Gateway als auch auf den Admin-Knoten konfiguriert.
Client-Typ	Der Typ der Clientanwendung, die diesen Endpunkt verwendet, entweder **S3** oder **Swift**.
Netzwerkprotokoll	Das Netzwerkprotokoll, das Clients beim Herstellen einer Verbindung mit diesem Endpunkt verwenden. • Wählen Sie **HTTPS** für eine 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 Nicht-Produktionsraster.

Verwaltungsschnittstelle

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt, der in der Tabelle auf der Seite „Load Balancer-Endpunkte“ angezeigt wird.
Hafen	Der StorageGRID -Port, den Sie für den Zugriff auf den Grid Manager, den Tenant Manager oder beide verwenden möchten. • Grid-Manager: **8443** • Mietermanager: **9443** • Sowohl Grid Manager als auch Tenant Manager: **443** **Hinweis**: Sie können diese voreingestellten Ports oder andere verfügbare Ports verwenden.
Schnittstellentyp	Wählen Sie das Optionsfeld für die StorageGRID -Schnittstelle aus, auf die Sie über diesen Endpunkt zugreifen.

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

1. Wählen Sie **Weiter**.

Auswählen eines Bindungsmodus

Schritte

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

   Einige Bindungsmodi sind entweder für Client-Endpunkte oder Management-Schnittstellen-Endpunkte verfügbar. Hier sind alle Modi für beide Endpunkttypen aufgelistet.

Modus	Beschreibung
Global (Standard für Client-Endpunkte)	Clients können über die IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, 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 die Erreichbarkeit dieses Endpunkts einschränken.
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder den entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die von Ihnen für die Endpunkte ausgewählten HA-Gruppen nicht überschneiden.
Knotenschnittstellen	Clients müssen die IP-Adressen (oder entsprechenden FQDNs) ausgewählter Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Knotentyp (nur Client-Endpunkte)	Je nach ausgewähltem 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-Knoten (Standard für Endpunkte der Verwaltungsschnittstelle)	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 für die Verwaltungsschnittstelle erstellen, sind nur Admin-Knoten zulässig.

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

   Wenn Sie Endpunkte der Verwaltungsschnittstelle erstellen, wählen Sie VIPs aus, die nur mit Admin-Knoten verknüpft sind.

3. Wenn Sie **Knotenschnittstellen** ausgewählt haben, wählen Sie eine oder mehrere Knotenschnittstellen für jeden Admin-Knoten oder Gateway-Knoten aus, den Sie diesem Endpunkt zuordnen möchten.
4. Wenn Sie **Knotentyp** ausgewählt haben, wählen Sie entweder „Admin-Knoten“, was sowohl den primären Admin-Knoten als auch alle nicht primären Admin-Knoten umfasst, oder „Gateway-Knoten“.

Steuern des Mandantenzugriffs

> Ein Management-Schnittstellen-Endpunkt kann den Mandantenzugriff nur steuern, wenn der Endpunkt über dieSchnittstellentyp des Tenant Managers .

Schritte

1. Wählen Sie für den Schritt **Mandantenzugriff** 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 verwenden, um auf ihre Buckets zuzugreifen.
Ausgewählte Mieter blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht verwenden, um auf ihre Buckets zuzugreifen. Alle anderen Mandanten können diesen Endpunkt verwenden.

2. Wenn Sie einen **HTTP**-Endpunkt erstellen, müssen Sie kein Zertifikat anhängen. Wählen Sie **Erstellen** aus, um den neuen Load Balancer-Endpunkt hinzuzufügen. Gehen Sie dann zuNach Abschluss .

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-Clients und dem Load Balancer-Dienst auf Admin-Knoten oder Gateway-Knoten.

   - **Zertifikat hochladen**. Wählen Sie diese Option, wenn Sie benutzerdefinierte Zertifikate hochladen möchten.
   - **Zertifikat erstellen**. Wählen Sie diese Option, wenn Sie über die zum Generieren eines benutzerdefinierten Zertifikats erforderlichen Werte verfügen.
   - **Verwenden Sie das StorageGRID S3-Zertifikat**. Wählen Sie diese Option, wenn Sie das globale S3-API-Zertifikat verwenden möchten, das auch für direkte Verbindungen zu Speicherknoten verwendet werden kann.

     Sie können diese Option nur auswählen, wenn Sie das standardmäßige S3-API-Zertifikat, das von der Grid-CA signiert ist, durch ein benutzerdefiniertes Zertifikat ersetzt haben, das von einer externen Zertifizierungsstelle signiert ist. Sehen "Konfigurieren von S3-API-Zertifikaten" .

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

Zertifikat hochladen

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatsdateien hoch:

- **Serverzertifikat**: Die benutzerdefinierte Serverzertifikatsdatei in PEM-Kodierung.
- **Privater Zertifikatsschlüssel**: Die benutzerdefinierte private Schlüsseldatei des Serverzertifikats(`.key`).

> Private EC-Schlüssel müssen mindestens 224 Bit lang sein. Private RSA-Schlüssel müssen mindestens 2048 Bit lang sein.

- **CA-Paket**: Eine einzelne optionale Datei, die die Zertifikate jeder zwischengeschalteten ausstellenden Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-codierten CA-Zertifikatsdateien enthalten, die in der Reihenfolge der Zertifikatskette aneinandergereiht sind.

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

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

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

Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat PEM kopieren** oder **CA-Paket PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

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

Zertifikat generieren

a. Wählen Sie **Zertifikat generieren**.

b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domänenname	Ein oder mehrere vollqualifizierte Domänennamen, die in das Zertifikat aufgenommen werden sollen. Verwenden Sie ein * als Platzhalter, um mehrere Domänennamen darzustellen.
IP	Eine oder mehrere IP-Adressen, die in das Zertifikat aufgenommen werden sollen.

Feld	Beschreibung
Betreff (optional)	X.509-Betreff oder Distinguished Name (DN) des Zertifikatsinhabers. Wenn in dieses Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domänennamen oder die erste IP-Adresse als allgemeinen Namen (CN) des Betreffs.
Gültigkeitstage	Anzahl der Tage nach der Erstellung, bis zu der das Zertifikat abläuft.
Hinzufügen von Schlüsselverwendungserweiterungen	Wenn ausgewählt (Standard und empfohlen), werden dem generierten Zertifikat Schlüsselverwendung und erweiterte Schlüsselverwendungserweiterungen hinzugefügt. Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels. **Hinweis**: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn die Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Generieren**.

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

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

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

   Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

e. Wählen Sie **Erstellen**.

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

Nach Abschluss

Schritte

1. Wenn Sie ein DNS verwenden, stellen Sie sicher, dass das DNS einen Datensatz enthält, um den vollqualifizierten Domänennamen (FQDN) von StorageGRID jeder IP-Adresse zuzuordnen, die Clients zum Herstellen von Verbindungen verwenden.

   Die IP-Adresse, die Sie in den DNS-Eintrag eingeben, hängt davon ab, ob Sie eine HA-Gruppe von Lastausgleichsknoten 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 über die IP-Adresse eines Gateway-Knotens oder Admin-Knotens eine Verbindung zum StorageGRID Load Balancer-Dienst her.

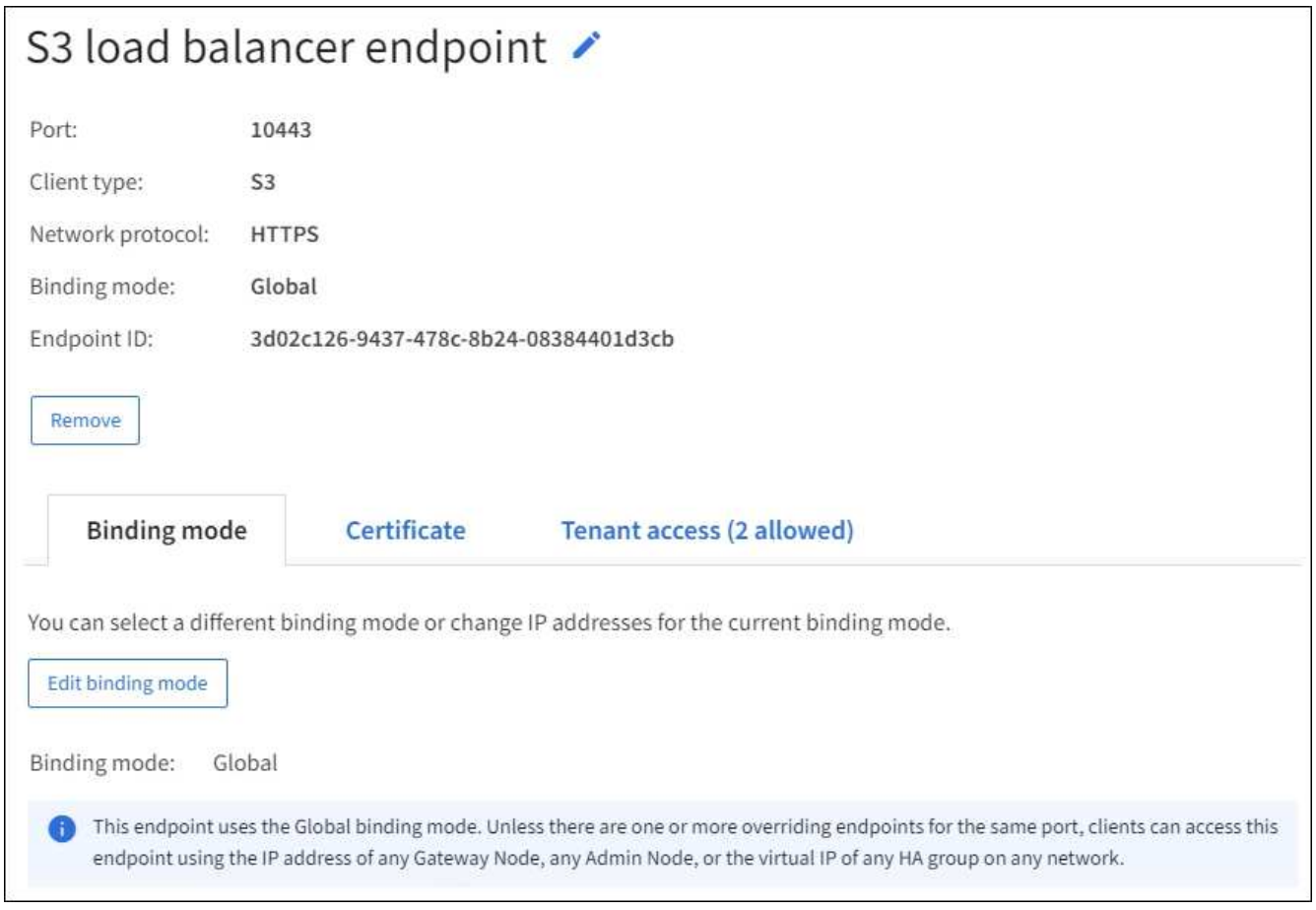
  Sie müssen außerdem sicherstellen, dass der DNS-Eintrag auf alle erforderlichen Endpunktdomänennamen verweist, einschließlich aller Platzhalternamen.

2. Stellen Sie S3-Clients die Informationen zur Verfügung, die zum Herstellen einer Verbindung mit dem Endpunkt erforderlich sind:
   - Portnummer
   - Vollqualifizierter Domänenname oder IP-Adresse
   - Alle erforderlichen Zertifikatsdetails

Anzeigen und Bearbeiten von Load Balancer-Endpunkten

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 zu allen Load Balancer-Endpunkten anzuzeigen, sehen Sie sich die Tabellen auf der Seite „Load Balancer-Endpunkte“ an.
- Um alle Details zu einem bestimmten Endpunkt anzuzeigen, einschließlich Zertifikatmetadaten, wählen Sie den Namen des Endpunkts in der Tabelle aus. Die angezeigten Informationen variieren je nach Endpunkttyp und Konfiguration.



- Um einen Endpunkt zu bearbeiten, verwenden Sie das Menü **Aktionen** auf der Seite „Load Balancer-Endpunkte“.

> Wenn Sie beim Bearbeiten des Ports eines Management-Schnittstellenendpunkts den Zugriff auf Grid Manager verlieren, aktualisieren Sie die URL und den Port, um den Zugriff wiederzuerlangen.

> Nach der Bearbeitung eines Endpunkts müssen Sie möglicherweise bis zu 15 Minuten warten, bis Ihre Änderungen auf alle Knoten angewendet werden.

Aufgabe	Menü „Aktionen“	Detailseite
Endpunktnamen bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** > **Endpunktnamen bearbeiten**. 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 **Aktionen** > **Endpunktport bearbeiten** 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 nach Bedarf. 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 nach Bedarf. 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**. c. Laden Sie ein neues benutzerdefiniertes Zertifikat hoch oder generieren Sie es, oder beginnen Sie bei Bedarf mit der Verwendung des globalen S3-Zertifikats. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte **Zertifikat**. c. Wählen Sie **Zertifikat bearbeiten**. d. Laden Sie ein neues benutzerdefiniertes Zertifikat hoch oder generieren Sie es, oder beginnen Sie bei Bedarf mit der Verwendung des globalen S3-Zertifikats. e. Wählen Sie **Änderungen speichern**.
Mandantenzugriff bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** > **Mandantenzugriff bearbeiten**. c. Wählen Sie eine andere Zugriffsoption, wählen Sie Mandanten aus der Liste aus oder entfernen Sie sie, oder tun Sie beides. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte **Mandantenzugriff**. c. Wählen Sie **Mandantenzugriff bearbeiten**. d. Wählen Sie eine andere Zugriffsoption, wählen Sie Mandanten aus der Liste aus oder entfernen Sie sie, oder tun Sie beides. e. Wählen Sie **Änderungen speichern**.

Entfernen von Load Balancer-Endpunkten

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

> Um Clientunterbrechungen zu vermeiden, aktualisieren Sie alle betroffenen S3-Clientanwendungen, 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. Denken Sie daran, auch alle erforderlichen Zertifikatsinformationen zu aktualisieren.

> Wenn Sie beim Entfernen eines Verwaltungsschnittstellen-Endpunkts den Zugriff auf Grid Manager verlieren, 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 von der Detailseite:
  a. Wählen Sie auf der Seite „Load Balancer“ den Endpunktnamen aus.
  b. Wählen Sie auf der Detailseite **Entfernen** aus.
  c. Wählen Sie **OK**.

Konfigurieren von S3-Endpunktdomänennamen

Um Anfragen im S3-Virtual-Hosting-Stil zu unterstützen, müssen Sie den Grid Manager verwenden, um die Liste der S3-Endpunktdomänennamen zu konfigurieren, mit denen S3-Clients eine Verbindung herstellen.

Die Verwendung einer IP-Adresse als Endpunktdomänenname wird nicht unterstützt. Zukünftige Versionen werden diese Konfiguration verhindern.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben bestätigt, dass kein Netz-Upgrade im Gange ist.

Nehmen Sie keine Änderungen an der Domänennamenkonfiguration vor, während ein Grid-Upgrade durchgeführt wird.

Informationen zu diesem Vorgang

Damit Clients S3-Endpunktdomänennamen verwenden können, müssen Sie alle folgenden Schritte ausführen:

- Verwenden Sie den Grid Manager, um die S3-Endpunktdomänennamen zum StorageGRID -System hinzuzufügen.
- Stellen Sie sicher, dass die"Zertifikat, das der Client für HTTPS-Verbindungen zu StorageGRID verwendet" ist für alle Domänennamen signiert, die der Client benötigt.

  Wenn der Endpunkt beispielsweise `s3.company.com` müssen Sie sicherstellen, dass das für HTTPS-Verbindungen verwendete Zertifikat die `s3.company.com` Endpunkt und der Platzhalter „Subject Alternative Name“ (SAN) des Endpunkts: `*.s3.company.com` .

- Konfigurieren Sie den vom Client verwendeten DNS-Server. Fügen Sie DNS-Einträge für die IP-Adressen ein, die Clients zum Herstellen von Verbindungen verwenden, und stellen Sie sicher, dass die Einträge auf alle erforderlichen S3-Endpunktdomänennamen verweisen, einschließlich aller Platzhalternamen.

Clients können sich mit StorageGRID über die IP-Adresse eines Gateway-Knotens, eines Admin-Knotens oder eines Storage-Knotens verbinden oder indem sie sich mit der virtuellen IP-Adresse einer Hochverfügbarkeitsgruppe verbinden. Sie sollten verstehen, wie Clientanwendungen eine Verbindung zum Grid herstellen, damit Sie die richtigen IP-Adressen in die DNS-Einträge aufnehmen.

Clients, die HTTPS-Verbindungen (empfohlen) zum Grid verwenden, können eines dieser Zertifikate verwenden:

- Clients, die eine Verbindung zu einem Load Balancer-Endpunkt herstellen, können für diesen Endpunkt ein benutzerdefiniertes Zertifikat verwenden. Jeder Load Balancer-Endpunkt kann so konfiguriert werden, dass er unterschiedliche S3-Endpunktdomänennamen erkennt.
- Clients, die eine Verbindung zu einem Load Balancer-Endpunkt oder direkt zu einem Speicherknoten herstellen, können das globale S3-API-Zertifikat so anpassen, dass alle erforderlichen S3-Endpunktdomänennamen enthalten sind.

> Wenn Sie keine S3-Endpunktdomänennamen hinzufügen und die Liste leer ist, wird die Unterstützung für Anfragen im virtuell gehosteten S3-Stil deaktiviert.

Fügen Sie einen S3-Endpunktdomänennamen hinzu

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **S3-Endpunktdomänennamen**.
2. Geben Sie den Domänennamen in das Feld **Domänenname 1** ein. Wählen Sie **Weiteren Domänennamen hinzufügen**, um weitere Domänennamen hinzuzufügen.
3. Wählen Sie **Speichern**.
4. Stellen Sie sicher, dass die von den Clients verwendeten Serverzertifikate mit den erforderlichen Domänennamen des S3-Endpunkts übereinstimmen.
   - Wenn Clients eine Verbindung zu einem Load Balancer-Endpunkt herstellen, der ein eigenes Zertifikat verwendet,"Aktualisieren Sie das dem Endpunkt zugeordnete Zertifikat" .
   - Wenn Clients eine Verbindung zu einem Load Balancer-Endpunkt herstellen, der das globale S3-API-Zertifikat verwendet, oder direkt zu Storage Nodes,"Aktualisieren Sie das globale S3-API-Zertifikat" .
5. Fügen Sie die erforderlichen DNS-Einträge hinzu, um sicherzustellen, dass Domänennamenanforderungen von Endpunkten aufgelöst werden können.

Ergebnis

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

Umbenennen eines S3-Endpunktdomänennamens

Wenn Sie einen von S3-Anwendungen verwendeten Namen ändern, schlagen Anfragen im virtuell gehosteten Stil fehl.

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **S3-Endpunktdomänennamen**.
2. Wählen Sie das Domänennamenfeld aus, das Sie bearbeiten möchten, und nehmen Sie die erforderlichen Änderungen vor.
3. Wählen Sie **Speichern**.
4. Wählen Sie **Ja**, um Ihre Änderung zu bestätigen.

Löschen eines S3-Endpunktdomänennamens

Wenn Sie einen von S3-Anwendungen verwendeten Namen entfernen, schlagen Anfragen im virtuell gehosteten Stil fehl.

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **S3-Endpunktdomänennamen**.
2. Wählen Sie das Löschsymbol neben dem Domänennamen.
3. Wählen Sie **Ja**, um den Löschvorgang zu bestätigen.

Ähnliche Informationen

- "Verwenden Sie die S3 REST-API"
- "IP-Adressen anzeigen"
- "Konfigurieren von Hochverfügbarkeitsgruppen"

Zusammenfassung: IP-Adressen und Ports für Clientverbindungen

Um Objekte zu speichern oder abzurufen, stellen S3-Clientanwendungen eine Verbindung zum Load Balancer-Dienst her, der auf allen Admin-Knoten und Gateway-Knoten enthalten ist, oder zum Local Distribution Router (LDR)-Dienst, der auf allen Speicherknoten enthalten ist.

Client-Anwendungen können über die IP-Adresse eines Grid-Knotens und die Portnummer des Dienstes auf diesem Knoten eine Verbindung zu StorageGRID herstellen. Optional können Sie Hochverfügbarkeitsgruppen (HA) von Lastausgleichsknoten erstellen, um hochverfügbare Verbindungen bereitzustellen, die virtuelle IP-Adressen (VIP) verwenden. Wenn Sie eine Verbindung zu StorageGRID über einen vollqualifizierten Domänennamen (FQDN) anstelle einer IP- oder VIP-Adresse herstellen möchten, können Sie DNS-Einträge konfigurieren.

Diese Tabelle fasst die verschiedenen Möglichkeiten zusammen, wie Clients eine Verbindung zu StorageGRID herstellen können, sowie die IP-Adressen und Ports, die für die einzelnen Verbindungstypen verwendet werden. Wenn Sie bereits Load Balancer-Endpunkte und Hochverfügbarkeitsgruppen (HA) erstellt haben, lesen SieWo finde ich IP-Adressen? um diese Werte im Grid Manager zu finden.

Wo die Verbindung hergestellt wird	Dienst, mit dem der Client eine Verbindung herstellt	IP-Adresse	Hafen
HA-Gruppe	Lastenausgleich	Virtuelle IP-Adresse einer HA-Gruppe	Dem Load Balancer-Endpunkt zugewiesener Port
Admin-Knoten	Lastenausgleich	IP-Adresse des Admin-Knotens	Dem Load Balancer-Endpunkt zugewiesener Port
Gateway-Knoten	Lastenausgleich	IP-Adresse des Gateway-Knotens	Dem Load Balancer-Endpunkt zugewiesener Port

Wo die Verbindung hergestellt wird	Dienst, mit dem der Client eine Verbindung herstellt	IP-Adresse	Hafen
Speicherknoten	LDR	IP-Adresse des Speicherknotens	Standard-S3-Ports: • HTTPS: 18082 • HTTP: 18084

Beispiel-URLs

Um eine Clientanwendung mit dem Load Balancer-Endpunkt einer HA-Gruppe von Gateway-Knoten zu verbinden, verwenden Sie eine URL mit der folgenden Struktur:

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

Wenn beispielsweise die virtuelle IP-Adresse der HA-Gruppe 192.0.2.5 und die Portnummer des Load Balancer-Endpunkts 10443 ist, könnte eine Anwendung die folgende URL verwenden, um eine Verbindung zu StorageGRID herzustellen:

`https://192.0.2.5:10443`

Wo finde ich IP-Adressen?

1. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .
2. So finden Sie die IP-Adresse eines Grid-Knotens:
   a. Wählen Sie **NODES**.
   b. Wählen Sie den Admin-Knoten, Gateway-Knoten oder Speicherknoten aus, zu dem Sie eine Verbindung herstellen möchten.
   c. Wählen Sie die Registerkarte **Übersicht**.
   d. Notieren Sie im Abschnitt „Knoteninformationen“ die IP-Adressen für den Knoten.
   e. Wählen Sie **Mehr anzeigen**, um IPv6-Adressen und Schnittstellenzuordnungen anzuzeigen.

      Sie können Verbindungen von Clientanwendungen zu jeder der IP-Adressen in der Liste herstellen:

      - **eth0:** Grid-Netzwerk
      - **eth1:** Admin-Netzwerk (optional)
      - **eth2:** Client-Netzwerk (optional)

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

3. So finden Sie die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe:
   a. Wählen Sie **KONFIGURATION** > **Netzwerk** > **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** > **Netzwerk** > **Load Balancer-Endpunkte**.

b. Notieren Sie sich die Portnummer für den Endpunkt, den Sie verwenden möchten.

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

c. Wählen Sie den Namen des Endpunkts aus der Tabelle aus.

d. Bestätigen Sie, dass der **Clienttyp** (S3) mit der Clientanwendung übereinstimmt, die den Endpunkt verwenden wird.