



Client-Verbindungen konfigurieren

StorageGRID

NetApp
March 12, 2025

Inhalt

Client-Verbindungen konfigurieren	1
S3-Client-Verbindungen konfigurieren	1
Konfigurationsaufgaben	1
Informationen, die zum Anhängen von StorageGRID an eine Client-Applikation erforderlich sind	2
Sicherheit für S3-Clients	3
Zusammenfassung	3
Wie StorageGRID Sicherheit für Client-Anwendungen bietet	4
Unterstützte Hashing- und Verschlüsselungsalgorithmen für TLS-Bibliotheken	5
Verwenden Sie den S3-Einrichtungsassistenten	5
Überlegungen und Anforderungen im S3-Setup-Assistenten	5
Rufen Sie den S3-Setup-Assistenten auf und vervollständigen Sie sie	6
Managen von HA-Gruppen	14
Was sind Hochverfügbarkeitsgruppen (High Availability Groups, HA-Gruppen)?	14
Wie werden HA-Gruppen verwendet?	17
Konfigurationsoptionen für HA-Gruppen	18
Konfigurieren Sie Hochverfügbarkeitsgruppen	20
Managen Sie den Lastausgleich	25
Überlegungen zum Lastausgleich	25
Konfigurieren von Load Balancer-Endpunkten	29
Konfigurieren Sie die Domännennamen des S3-Endpunkts	40
Fügen Sie einen S3-Endpunkt-Domännennamen hinzu	41
Benennen Sie einen S3-Endpunkt-Domännennamen um	41
Löschen Sie einen S3-Endpunkt-Domännennamen	41
Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen	42
Beispiel-URLs	43
Wo finden Sie IP-Adressen	43

Client-Verbindungen konfigurieren

S3-Client-Verbindungen konfigurieren

Als Grid-Administrator managen Sie die Konfigurationsoptionen, die steuern, wie S3-Client-Applikationen zum Speichern und Abrufen von Daten mit Ihrem StorageGRID System verbunden sind.



Swift-Details wurden aus dieser Version der doc-Site entfernt. Siehe "[StorageGRID 11.8: Konfigurieren Sie S3- und Swift-Client-Verbindungen](#)".

Konfigurationsaufgaben

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

Erforderliche Aufgaben

Sie müssen Folgendes erhalten:

- IP-Adressen
- Domain-Namen
- SSL-Zertifikat

Optionale Aufgaben

Optional konfigurieren:

- 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-Einrichtungsassistenten verwenden oder jede StorageGRID-Einheit manuell konfigurieren.

Verwenden Sie den S3-Einrichtungsassistenten

Befolgen Sie die Schritte im S3-Einrichtungsassistenten.

Manuell konfigurieren

1. Erstellen Sie eine Hochverfügbarkeitsgruppe
2. Lastausgleichsendpunkt erstellen
3. Erstellen eines Mandantenkontos
4. Erstellen von Buckets und Zugriffsschlüsseln
5. Konfigurieren Sie die ILM-Regel und -Richtlinie

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

DNS-Einträge, um IP-Adressen mit beliebigen Domännennamen zu verknüpfen, die Sie verwenden möchten.

Führen Sie bei Bedarf zusätzliche Anwendungseinstellungen durch.

2. Laufende Aufgaben in der Applikation und in StorageGRID werden durchgeführt, um Objekt-Storage über einen längeren Zeitraum zu managen und zu überwachen.

Informationen, die zum Anhängen von StorageGRID an eine Client-Applikation erforderlich sind

Bevor Sie StorageGRID an eine S3-Client-Anwendung anhängen können, müssen Sie die Konfigurationsschritte in StorageGRID ausführen und einen bestimmten Wert erhalten.

Welche Werte brauche ich?

In der folgenden Tabelle sind die Werte aufgeführt, die Sie in StorageGRID konfigurieren müssen und bei denen diese Werte von der S3-Anwendung und dem DNS-Server verwendet werden.

Wert	Wobei der Wert konfiguriert ist	Wo Wert verwendet wird
Virtuelle IP-Adressen (VIP)	StorageGRID > HA-Gruppe	DNS-Eintrag
Port	StorageGRID > Endpunkt des Load Balancer	Client-Anwendung
SSL-Zertifikat	StorageGRID > Endpunkt des Load Balancer	Client-Anwendung
Servername (FQDN)	StorageGRID > Endpunkt des Load Balancer	<ul style="list-style-type: none">• Client-Anwendung• DNS-Eintrag
S3 Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel	StorageGRID > Mandant und Bucket	Client-Anwendung
Bucket/Container-Name	StorageGRID > Mandant und Bucket	Client-Anwendung

Wie erhalte ich diese Werte?

Je nach Ihren Anforderungen können Sie eine der folgenden Möglichkeiten nutzen, um die benötigten Informationen zu erhalten:

- **Verwenden Sie die "S3-Einrichtungsassistent"**. Der S3-Einrichtungsassistent unterstützt Sie beim schnellen Konfigurieren der erforderlichen Werte in StorageGRID und gibt eine oder zwei Dateien aus, die Sie bei der Konfiguration der S3-Anwendung verwenden können. Der Assistent führt Sie durch die erforderlichen Schritte und stellt sicher, dass Ihre Einstellungen den StorageGRID Best Practices entsprechen.



Wenn Sie eine S3-Applikation konfigurieren, wird die Verwendung des S3-Setup-Assistenten von empfohlen, es sei denn, Sie verfügen über besondere Anforderungen oder Ihre Implementierung erfordert eine umfangreiche Anpassung.

- **Verwenden Sie die "FabricPool Setup-Assistent"**. Ähnlich wie der S3-Einrichtungsassistent unterstützt Sie der FabricPool-Einrichtungsassistent bei der schnellen Konfiguration der erforderlichen Werte und gibt eine Datei aus, die Sie bei der Konfiguration eines FabricPool-Cloud-Tiers in ONTAP verwenden können.



Wenn Sie StorageGRID als Objekt-Storage-System für eine FabricPool Cloud-Tier nutzen möchten, empfiehlt sich die Verwendung des FabricPool Setup-Assistenten, es sei denn, Sie haben besondere Anforderungen oder Ihre Implementierung erfordert erhebliche Anpassungen.

- **Elemente manuell konfigurieren.** Wenn Sie eine Verbindung zu einer S3-Anwendung herstellen und den S3-Einrichtungsassistenten nicht verwenden möchten, können Sie die erforderlichen Werte abrufen, indem Sie die Konfiguration manuell durchführen. Führen Sie hierzu folgende Schritte aus:
 - a. Konfigurieren Sie die HA-Gruppe (High Availability, Hochverfügbarkeit), die Sie für die S3-Applikation verwenden möchten. Siehe "[Konfigurieren Sie Hochverfügbarkeitsgruppen](#)".
 - b. Erstellen Sie den Load Balancer-Endpunkt, den die S3-Applikation verwenden wird. Siehe "[Konfigurieren von Load Balancer-Endpunkten](#)".
 - c. Erstellen Sie das Mandantenkonto, das die S3-Anwendung verwenden wird. Siehe "[Erstellen Sie ein Mandantenkonto](#)".
 - d. Melden Sie sich für einen S3-Mandanten beim Mandantenkonto an und generieren Sie für jeden Benutzer, der auf die Applikation zugreift, eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel. Siehe "[Erstellen Sie Ihre eigenen Zugriffsschlüssel](#)".
 - e. Erstellen Sie einen oder mehrere S3-Buckets innerhalb des Mandantenkontos. Für S3 siehe "[S3-Bucket erstellen](#)".
 - f. Um Anweisungen zur Platzierung von Objekten, die zu dem neuen Mandanten oder Bucket/Container gehören, hinzuzufügen, erstellen Sie eine neue ILM-Regel und aktivieren Sie zur Verwendung dieser Regel eine neue ILM-Richtlinie. Siehe "[ILM-Regel erstellen](#)" und "[ILM-Richtlinie erstellen](#)".

Sicherheit für S3-Clients

StorageGRID-Mandantenkonten verwenden S3-Client-Applikationen, um Objektdaten in StorageGRID zu speichern. Überprüfen Sie die Sicherheitsmaßnahmen, die für Client-Anwendungen implementiert wurden.

Zusammenfassung

In der folgenden Liste wird zusammengefasst, wie Sicherheit für die S3-REST-API implementiert wird:

Verbindungssicherheit

TLS

Serverauthentifizierung

X.509-Serverzertifikat, das von der System-CA oder vom Administrator zur Verfügung gestellten benutzerdefinierten Serverzertifikat unterzeichnet wurde

Client-Authentifizierung

Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel für das S3-Konto

Client-Autorisierung

Eigentümerschaft von Buckets und alle anwendbaren Zugriffssteuerungsrichtlinien

Wie StorageGRID Sicherheit für Client-Anwendungen bietet

S3-Client-Applikationen können sich mit dem Load Balancer-Service auf Gateway-Nodes oder Admin-Nodes oder direkt mit Storage-Nodes verbinden.

- Clients, die sich mit dem Load Balancer-Dienst verbinden, können HTTPS oder HTTP verwenden, je nachdem, wie Sie ["Konfigurieren Sie den Endpunkt des Load Balancer"](#).

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

HTTP bietet eine weniger sichere, unverschlüsselte Kommunikation und sollte nur für nicht-Produktions- oder Testraster verwendet werden.

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

HTTPS ist der Standardwert und wird empfohlen.

HTTP bietet eine weniger sichere, unverschlüsselte Kommunikation, kann aber optional ["Aktiviert"](#) für nicht-Produktions- oder Testraster eingesetzt werden.

- Die Kommunikation zwischen StorageGRID und dem Client wird über TLS verschlüsselt.
- Die Kommunikation zwischen dem Load Balancer-Service und den Speicherknoten innerhalb des Grid wird verschlüsselt, ob der Load Balancer-Endpunkt für die Annahme von HTTP- oder HTTPS-Verbindungen konfiguriert ist.
- Clients müssen an StorageGRID bereitstellen ["HTTP-Authentifizierungsheader"](#), um REST-API-Operationen durchführen zu können.

Sicherheitszertifikate und Clientanwendungen

Clientanwendungen können in jedem Fall 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 hat sein eigenes Zertifikat—entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein Zertifikat, das der Grid-Administrator beim Konfigurieren des Endpunkts in StorageGRID generiert hat.

Siehe ["Überlegungen zum Lastausgleich"](#).

- Wenn Client-Anwendungen eine direkte Verbindung zu einem Speicher-Node herstellen, verwenden sie entweder die vom System generierten Serverzertifikate, die bei der Installation des StorageGRID-Systems für Speicher-Nodes generiert wurden (die von der Systemzertifikatbehörde signiert werden). Oder ein einzelnes benutzerdefiniertes Serverzertifikat, das von einem Grid-Administrator für das Grid bereitgestellt wird. Siehe ["Fügen Sie ein benutzerdefiniertes S3-API-Zertifikat hinzu"](#).

Die Clients sollten so konfiguriert werden, dass sie der Zertifizierungsstelle vertrauen, die unabhängig davon, welches Zertifikat sie zum Erstellen von TLS-Verbindungen verwenden, unterzeichnet hat.

Unterstützte Hashing- und Verschlüsselungsalgorithmen für TLS-Bibliotheken

Das StorageGRID-System unterstützt eine Reihe von Cipher-Suites, die Client-Anwendungen beim Einrichten einer TLS-Sitzung verwenden können. Um Chiffren zu konfigurieren, gehen Sie zu **CONFIGURATION > Security > Security settings** und wählen **TLS und SSH Policies** aus.

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-Einrichtungsassistenten

Überlegungen und Anforderungen im S3-Setup-Assistenten

Sie können mit dem S3-Einrichtungsassistenten StorageGRID als Objekt-Storage-System für eine S3-Applikation konfigurieren.

Wann der S3-Einrichtungsassistent verwendet werden soll

Der S3-Einrichtungsassistent führt Sie durch jeden Schritt bei der Konfiguration von StorageGRID für die Verwendung mit einer S3-Applikation. Im Rahmen der Ausführung des Assistenten laden Sie Dateien herunter, mit denen Sie Werte in die S3-Anwendung eingeben können. Mit dem Assistenten konfigurieren Sie Ihr System schneller und stellen sicher, dass Ihre Einstellungen den StorageGRID Best Practices entsprechen.

Wenn Sie über den verfügen "[Root-Zugriffsberechtigung](#)", können Sie den S3-Einrichtungsassistenten abschließen, wenn Sie den StorageGRID-Grid-Manager verwenden, oder Sie können den Assistenten zu einem späteren Zeitpunkt aufrufen und abschließen. Je nach Ihren Anforderungen können Sie auch einige oder alle erforderlichen Elemente manuell konfigurieren und dann mithilfe des Assistenten die Werte zusammenstellen, die eine S3-Anwendung benötigt.

Bevor Sie den Assistenten verwenden

Vergewissern Sie sich vor der Verwendung des Assistenten, dass Sie diese Voraussetzungen erfüllt haben.

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

Wenn Sie eine HA-Gruppe (High Availability, Hochverfügbarkeit) konfigurieren, wissen Sie, mit welchen Nodes die S3-Applikation eine Verbindung herstellen und welches StorageGRID-Netzwerk verwendet wird. Sie wissen auch, welche Werte für das Subnetz CIDR, die Gateway-IP-Adresse und die virtuelle IP (VIP)-Adresse eingegeben werden sollen.

Wenn Sie planen, einen virtuellen LAN zur Trennung des Datenverkehrs von der S3-Anwendung zu verwenden, haben Sie die VLAN-Schnittstelle bereits konfiguriert. Siehe "[Konfigurieren Sie die VLAN-Schnittstellen](#)".

Konfigurieren Sie Identity Federation und SSO

Wenn Sie planen, Identity Federation oder Single Sign-On (SSO) für Ihr StorageGRID-System zu verwenden, haben Sie diese Funktionen aktiviert. Sie wissen auch, welche föderierte Gruppe Root-Zugriff

für das Mandantenkonto haben soll, das die S3-Anwendung verwenden wird. Siehe ["Verwenden Sie den Identitätsverbund"](#) und ["Konfigurieren Sie Single Sign-On"](#).

Abrufen und Konfigurieren von Domänennamen

Sie wissen, welcher vollständig qualifizierte Domänenname (FQDN) für StorageGRID verwendet werden soll. DNS-Einträge (Domain Name Server) weisen diesen FQDN den virtuellen IP-Adressen (VIP) der HA-Gruppe zu, die Sie mit dem Assistenten erstellen.

Wenn Sie Anforderungen im virtuellen gehosteten Stil von S3 verwenden möchten, sollten Sie über verfügen ["Domänennamen des S3-Endpunkts wurden konfiguriert"](#). Die Verwendung von Anforderungen im virtuellen Hosted-Stil wird empfohlen.

Anforderungen für Load Balancer und Sicherheitszertifikate prüfen

Wenn Sie den StorageGRID Load Balancer einsetzen möchten, haben Sie die allgemeinen Überlegungen zum Lastausgleich besprochen. Sie verfügen über die hochgeladenen Zertifikate oder die Werte, die Sie zum Generieren eines Zertifikats benötigen.

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

Konfigurieren Sie alle Verbindungen des Grid-Verbunds

Wenn Sie es dem S3-Mandanten erlauben möchten, Kontodaten zu klonen und Bucket-Objekte mithilfe einer Grid-Federation-Verbindung in ein anderes Grid zu replizieren, bestätigen Sie Folgendes, bevor Sie den Assistenten starten:

- Sie haben ["Grid Federation-Verbindung konfiguriert"](#).
- Der Status der Verbindung lautet **connected**.
- Sie haben Root-Zugriffsberechtigung.

Rufen Sie den S3-Setup-Assistenten auf und vervollständigen Sie sie

Sie können den S3-Einrichtungsassistenten verwenden, um StorageGRID für die Verwendung mit einer S3-Applikation zu konfigurieren. Der Einrichtungsassistent bietet die Werte, die die Anwendung benötigt, um auf einen StorageGRID-Bucket zuzugreifen und Objekte zu speichern.

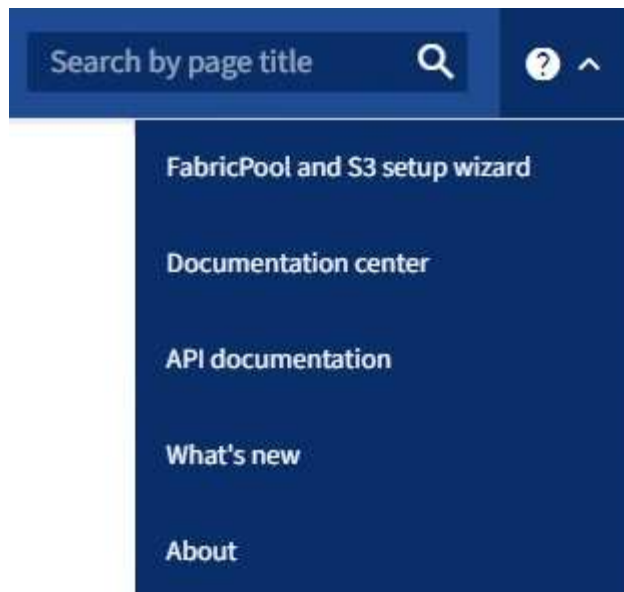
Bevor Sie beginnen

- Sie haben die ["Root-Zugriffsberechtigung"](#).
- Sie haben die zur Verwendung des Assistenten überprüft ["Überlegungen und Anforderungen"](#).

Greifen Sie auf den Assistenten zu

Schritte

1. Melden Sie sich mit einem beim Grid-Manager an ["Unterstützter Webbrowser"](#).
2. Wenn das Banner **FabricPool and S3 Setup Wizard** auf dem Dashboard angezeigt wird, wählen Sie den Link im Banner aus. Wenn das Banner nicht mehr angezeigt wird, wählen Sie in der Kopfzeile des Grid-Managers das Hilfesymbol aus und wählen Sie **FabricPool und S3-Setup-Assistent** aus.



3. Wählen Sie im Abschnitt S3-Anwendung der Seite FabricPool und S3-Setup-Assistent **Jetzt konfigurieren** aus.

Schritt 1 von 6: Konfigurieren Sie die HA-Gruppe

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

Sie können eine HA-Gruppe verwenden, um die S3 Datenverbindungen verfügbar zu halten. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload mit geringen Auswirkungen auf den S3-Betrieb managen.

Weitere Informationen zu dieser Aufgabe finden Sie unter "[Management von Hochverfügbarkeitsgruppen](#)".

Schritte

1. Wenn Sie einen externen Load Balancer verwenden möchten, müssen Sie keine HA-Gruppe erstellen. Wählen Sie **diesen Schritt überspringen** und gehen Sie zu [Schritt 2 von 6: Konfigurieren Sie den Load Balancer-Endpunkt](#).
2. Um den StorageGRID Load Balancer zu verwenden, können Sie eine neue HA-Gruppe erstellen oder eine vorhandene HA-Gruppe verwenden.

Erstellen Sie eine HA-Gruppe

- Um eine neue HA-Gruppe zu erstellen, wählen Sie **HA-Gruppe erstellen**.
- Füllen Sie für den Schritt **Enter Details** die folgenden Felder aus.

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

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

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

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

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

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

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

Wenn die HA-Gruppe mehr als eine Schnittstelle enthält und die aktive Schnittstelle ausfällt, werden die virtuellen IP-Adressen (VIP-Adressen) zur ersten Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. Wenn diese Schnittstelle ausfällt, wechseln die VIP-Adressen zur nächsten Backup-Schnittstelle usw. Wenn Fehler behoben sind, werden die VIP-Adressen auf die Schnittstelle mit der höchsten Priorität zurückverschoben.

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

Feld	Beschreibung
Subnetz-CIDR	Die Adresse des VIP-Subnetzes in CIDR-Notation — eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetz-Länge (0-32). Die Netzwerkadresse darf keine Host-Bits festgelegt haben. `192.16.0.0/22` Beispiel: .
Gateway-IP-Adresse (optional)	Wenn sich die S3-IP-Adressen für den Zugriff auf StorageGRID nicht im selben Subnetz wie die StorageGRID-VIP-Adressen befinden, geben Sie die lokale StorageGRID-VIP-Gateway-IP-Adresse ein. Die IP-Adresse des lokalen Gateways muss sich im VIP-Subnetz befinden.

Feld	Beschreibung
Virtuelle IP-Adresse	<p>Geben Sie mindestens eine und nicht mehr als zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden.</p> <p>Mindestens eine Adresse muss IPv4 sein. Optional können Sie weitere IPv4- und IPv6-Adressen angeben.</p>

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

g. Wählen Sie **Weiter**, um zum Schritt Load Balancer zu gelangen.

Verwenden Sie die vorhandene HA-Gruppe

a. Um eine vorhandene HA-Gruppe zu verwenden, wählen Sie den Namen der HA-Gruppe aus **Select an HA Group** aus.

b. Wählen Sie **Weiter**, um zum Schritt Load Balancer zu gelangen.

Schritt 2 von 6: Konfigurieren Sie den Load Balancer-Endpunkt

StorageGRID verwendet einen Load Balancer für das Management des Workloads aus Client-Applikationen. Load Balancing maximiert Geschwindigkeit und Verbindungskapazität über mehrere Storage Nodes hinweg.

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

Weitere Informationen zu dieser Aufgabe finden Sie unter "[Überlegungen zum Lastausgleich](#)".

Um den StorageGRID Load Balancer Service zu verwenden, wählen Sie die Registerkarte **StorageGRID Load Balancer** aus und erstellen oder wählen Sie dann den gewünschten Load Balancer-Endpunkt aus. Um einen externen Load Balancer zu verwenden, wählen Sie die Registerkarte **External Load Balancer** und geben Sie Details zum System an, das Sie bereits konfiguriert haben.

Endpoint erstellen

Schritte

1. Um einen Load Balancer-Endpoint zu erstellen, wählen Sie **Endpoint erstellen**.
2. Füllen Sie für den Schritt **Enter Endpoint Details** die folgenden Felder aus.

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpoint.
Port	<p>Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist für den ersten erstellten Endpoint standardmäßig auf 10433 eingestellt, Sie können jedoch jeden nicht verwendeten externen Port eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpoint nur auf Gateway-Nodes konfiguriert, da diese Ports auf Admin-Nodes reserviert sind.</p> <p>Hinweis: von anderen Netzdiensten verwendete Ports sind nicht erlaubt. Siehe "Referenz für Netzwerk-Ports".</p>
Client-Typ	Muss S3 sein.
Netzwerkprotokoll	<p>Wählen Sie HTTPS.</p> <p>Hinweis: Die Kommunikation mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen.</p>

3. Geben Sie für den Schritt **Bindungsmodus auswählen** den Bindungsmodus an. Der Bindungsmodus steuert, wie der Zugriff auf den Endpoint über eine beliebige IP-Adresse oder über spezifische IP-Adressen und Netzwerkschnittstellen erfolgt.

Modus	Beschreibung
Global (Standard)	<p>Clients können über die IP-Adresse eines beliebigen Gateway-Node oder Admin-Node, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpoint zugreifen.</p> <p>Verwenden Sie die Global-Einstellung (Standard), es sei denn, Sie müssen die Zugriffsmöglichkeiten dieses Endpoints einschränken.</p>
Virtuelle IPs von HA-Gruppen	<p>Clients müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpoint zuzugreifen.</p> <p>Endpoints mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überlappen.</p>

Modus	Beschreibung
Node-Schnittstellen	Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Node-Typ	Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.

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

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt für den Zugriff auf ihre Buckets verwenden.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Dieser Endpunkt kann von allen anderen Mandanten verwendet werden.

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

Feld	Beschreibung
Zertifikat hochladen (empfohlen)	Verwenden Sie diese Option, um ein CA-signiertes Serverzertifikat, einen privaten Zertifikatschlüssel und ein optionales CA-Paket hochzuladen.
Zertifikat wird generiert	Verwenden Sie diese Option, um ein selbstsigniertes Zertifikat zu generieren. Einzelheiten dazu finden Sie unter " Konfigurieren von Load Balancer-Endpunkten ".
StorageGRID S3-Zertifikat verwenden	Verwenden Sie diese Option nur, wenn Sie bereits eine benutzerdefinierte Version des globalen StorageGRID-Zertifikats hochgeladen oder generiert haben. Weitere Informationen finden Sie unter " Konfigurieren Sie S3-API-Zertifikate ".

6. Wählen Sie **Finish**, um zum S3-Setup-Assistenten zurückzukehren.

7. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.



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

Verwenden Sie den vorhandenen Endpunkt des Load Balancer

Schritte

1. Um einen vorhandenen Endpunkt zu verwenden, wählen Sie seinen Namen aus dem **Select a Load Balancer Endpunkt** aus.
2. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.

Externen Load Balancer verwenden

Schritte

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

Feld	Beschreibung
FQDN	Der vollständig qualifizierte Domänenname (FQDN) des externen Load Balancer.
Port	Die Portnummer, die die S3-Anwendung für die 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 Mandanten- und Bucket-Schritt zu gelangen.

Schritt 3 von 6: Erstellen Sie einen Mandanten und Bucket

Ein Mandant ist eine Einheit, die S3-Applikationen zum Speichern und Abrufen von Objekten in StorageGRID verwenden kann. Jeder Mandant verfügt über eigene Benutzer, Zugriffsschlüssel, Buckets, Objekte und bestimmte Funktionen.

Ein Bucket ist ein Container, mit dem die Objekte und Objektmetadaten eines Mandanten gespeichert werden können. Obwohl Mandanten möglicherweise über viele Buckets verfügen, hilft Ihnen der Assistent dabei, auf schnelle und einfache Weise einen Mandanten und einen Bucket zu erstellen. Wenn Sie zu einem späteren Zeitpunkt Buckets hinzufügen oder Optionen festlegen müssen, können Sie den Tenant Manager verwenden.

Weitere Informationen zu dieser Aufgabe finden Sie unter ["Erstellen eines Mandantenkontos"](#) und ["S3-Bucket erstellen"](#).

Schritte

1. Geben Sie einen Namen für das Mandantenkonto ein.

Mandantennamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, numerische Konto-ID.

2. Definieren Sie den Root-Zugriff für das Mandantenkonto, je nachdem, ob Ihr StorageGRID-System ["Identitätsföderation"](#), ["Single Sign On \(SSO\)"](#) oder beides verwendet.

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

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

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

Wählen Sie diese Option aus, wenn der einzige Benutzer für den Mandanten der Root-Benutzer ist. Wenn andere Benutzer diesen Mandanten verwenden, konfigurieren Sie "[Verwenden Sie Tenant Manager](#)" Schlüssel und Berechtigungen.

4. Wenn Sie jetzt einen Bucket für diesen Mandanten erstellen möchten, wählen Sie **Create Bucket for this Tenant** aus.



Wenn S3 Object Lock für das Raster aktiviert ist, ist für den in diesem Schritt erstellten Bucket die S3 Object Lock nicht aktiviert. Wenn Sie einen S3-Objektsperre-Bucket für diese S3-Applikation verwenden müssen, wählen Sie jetzt nicht, um einen Bucket zu erstellen. Verwenden Sie stattdessen Tenant Manager zu "[Erstellen Sie den Bucket](#)" einem späteren Zeitpunkt.

- a. Geben Sie den Namen des Buckets ein, den die S3-Applikation verwendet. `s3-bucket` Beispiel: .

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

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


Verwenden Sie die Standardregion (`us-east-1`), es sei denn, Sie werden zukünftig 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 zum Herunterladen von Daten können Sie eine oder zwei Dateien herunterladen, um die Details zu dem zu speichern, was Sie gerade konfiguriert haben.

Schritte

- Wenn Sie **Root-Benutzer S3-Zugriffsschlüssel automatisch erstellen** ausgewählt haben, führen Sie einen oder beide der folgenden Schritte aus:
 - Wählen Sie **Zugriffsschlüssel herunterladen**, um eine Datei herunterzuladen `.csv`, die den Namen des Mandantenkontos, die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel enthält.
 - Wählen Sie das Kopiersymbol () , um die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel in die Zwischenablage zu kopieren.

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



Schließen Sie diese Seite erst, wenn Sie beide Zugriffsschlüssel kopiert haben. Die Tasten sind nach dem Schließen dieser Seite nicht mehr verfügbar. Speichern Sie diese Informationen an einem sicheren Ort, da sie zum Abrufen von Daten von Ihrem StorageGRID-System verwendet werden können.

4. Wenn Sie dazu aufgefordert werden, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Schlüssel heruntergeladen oder kopiert haben.
5. Wählen Sie **Weiter**, um zur ILM-Regel und zum Richtlinien-schritt zu gelangen.

Schritt 5 von 6: Prüfen Sie die ILM-Regel und die ILM-Richtlinie für S3

Informationen Lifecycle Management-Regeln (ILM) steuern die Platzierung, Dauer und das Aufnahmeverhalten aller Objekte in Ihrem StorageGRID System. Mit der bei StorageGRID enthaltenen ILM-Richtlinie werden zwei replizierte Kopien aller Objekte erstellt. Diese Richtlinie ist gültig, bis Sie mindestens eine neue Richtlinie aktivieren.

Schritte

1. Überprüfen Sie die Informationen auf der Seite.
2. Wenn Sie bestimmte Anweisungen für die Objekte hinzufügen möchten, die zum neuen Mandanten oder Bucket gehören, erstellen Sie eine neue Regel und eine neue Richtlinie. Siehe "[ILM-Regel erstellen](#)" und "[Verwenden Sie 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 die nächsten Schritte verstehen.
5. Wählen Sie **Weiter**, um zu **Zusammenfassung** zu gelangen.

Schritt 6 von 6: Zusammenfassung überprüfen

Schritte

1. Überprüfen Sie die Zusammenfassung.
2. Notieren Sie sich in den nächsten Schritten die Details, die die zusätzliche Konfiguration beschreiben, die möglicherweise erforderlich ist, bevor Sie eine Verbindung zum S3-Client herstellen. Wenn Sie beispielsweise **als root anmelden** auswählen, gelangen Sie zum Tenant Manager, wo Sie Mandantenbenutzer hinzufügen, zusätzliche Buckets erstellen und Bucket-Einstellungen aktualisieren können.
3. Wählen Sie **Fertig**.
4. Konfigurieren Sie die Anwendung mit der Datei, die Sie von StorageGRID heruntergeladen haben, oder mit den manuell erhaltenen Werten.

Managen von HA-Gruppen

Was sind Hochverfügbarkeitsgruppen (High Availability Groups, HA-Gruppen)?

Hochverfügbarkeitsgruppen (HA-Gruppen) bieten hochverfügbare Datenverbindungen für

S3-Clients und hochverfügbare Verbindungen zu Grid Manager und Tenant Manager.

Die Netzwerkschnittstellen mehrerer Admin- und Gateway-Nodes können in einer HA-Gruppe (High Availability, Hochverfügbarkeit) gruppieren. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload verwalten.

Jede HA-Gruppe bietet Zugriff auf die Shared Services auf den ausgewählten Nodes.

- HA-Gruppen, die Gateway-Nodes, Admin-Nodes oder beide umfassen, stellen hochverfügbare Datenverbindungen für S3-Clients bereit.
- HA-Gruppen, die nur Admin-Nodes enthalten, bieten hochverfügbare Verbindungen zum Grid Manager und dem Mandanten-Manager.
- Eine HA-Gruppe, die nur Services Appliances und VMware-basierte Software Nodes umfasst "[S3-Mandanten, die S3 Select nutzen](#)", kann hochverfügbare Verbindungen für bereitstellen. HA-Gruppen werden empfohlen, wenn S3 Select verwendet wird, jedoch nicht erforderlich.

Wie erstellen Sie eine HA-Gruppe?

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



Sie können einer HA-Gruppe keine Schnittstelle hinzufügen, wenn ihr eine DHCP-zugewiesene IP-Adresse zugewiesen ist.

2. Sie geben an, dass die primäre Schnittstelle sein soll. 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 10 virtuelle IP-Adressen (VIP) zu. Client-Anwendungen können eine dieser VIP-Adressen verwenden, um eine Verbindung zu StorageGRID herzustellen.

Anweisungen hierzu finden Sie unter "[Konfigurieren Sie Hochverfügbarkeitsgruppen](#)".

Was ist die aktive Schnittstelle?

Im normalen Betrieb 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 sich Clients mit einer beliebigen VIP-Adresse für die Gruppe verbinden. Das heißt, während des normalen Betriebs ist die primäre Schnittstelle die „aktive“ Schnittstelle für die Gruppe.

Ebenso fungieren alle Schnittstellen mit niedriger Priorität für die HA-Gruppe im normalen Betrieb als „Backup“-Schnittstellen. Diese Backup-Schnittstellen werden nur dann verwendet, wenn die primäre (derzeit aktive) Schnittstelle nicht mehr verfügbar ist.

Anzeigen des aktuellen HA-Gruppen-Status eines Node

Um zu ermitteln, ob ein Node einer HA-Gruppe zugewiesen ist und seinen aktuellen Status ermittelt, wählen Sie **NODES > Node** aus.

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 Node in der HA-Gruppe:

- **Aktiv:** Die HA-Gruppe wird derzeit auf diesem Knoten gehostet.
- **Backup:** Die HA-Gruppe benutzt derzeit nicht diesen Knoten; dies ist ein Backup Interface.
- **Angehalten:** Die HA-Gruppe kann nicht auf diesem Knoten gehostet werden, da der Dienst hohe Verfügbarkeit (keepalibed) manuell angehalten wurde.
- **Fault:** Die HA-Gruppe kann nicht auf diesem Knoten gehostet werden, weil einer oder mehrere der folgenden:
 - Der Lastverteilungsservice (nginx-gw) wird auf dem Knoten nicht ausgeführt.
 - Die eth0- oder VIP-Schnittstelle des Node ist nicht aktiv.
 - Der Node ist ausgefallen.

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

DC1-ADM1 (Primary Admin Node) [🔗](#)

Overview Hardware Network Storage Load balancer Tasks

Node information [?](#)

Name: DC1-ADM1

Type: Primary Admin Node

ID: ce00d9c8-8a79-4742-bdef-c9c658db5315

Connection state: ✔ Connected

Software version: 11.6.0 (build 20211207.1804.614bc17)

HA groups: Admin clients (Active)
FabricPool clients (Backup)

IP addresses: 172.16.1.225 - eth0 (Grid Network)
10.224.1.225 - eth1 (Admin Network)
47.47.0.2, 47.47.1.225 - eth2 (Client Network)

[Show additional IP addresses](#) ▼

Was geschieht, wenn die aktive Schnittstelle ausfällt?

Die Schnittstelle, die derzeit die VIP-Adressen hostet, ist die aktive Schnittstelle. Wenn die HA-Gruppe mehrere Schnittstellen umfasst und die aktive Schnittstelle ausfällt, verschieben sich die VIP-Adressen auf die erste verfügbare Backup-Schnittstelle in der Prioritätsreihenfolge. Wenn diese Schnittstelle ausfällt, wechseln die VIP-Adressen zur nächsten verfügbaren Backup-Schnittstelle usw.

Ein Failover kann aus einem der folgenden Gründe ausgelöst werden:

- Der Node, auf dem die Schnittstelle konfiguriert ist, schaltet sich aus.
- Der Node, auf dem die Schnittstelle konfiguriert ist, verliert mindestens 2 Minuten lang die Verbindung zu allen anderen Nodes.

- Die aktive Schnittstelle ausfällt.
- Der Lastverteiler-Dienst wird angehalten.
- Der High Availability Service stoppt.



Der Failover wird möglicherweise nicht durch Netzwerkausfälle außerhalb des Node ausgelöst, der die aktive Schnittstelle hostet. Ebenso wird Failover nicht von den Diensten für den Grid Manager oder den Tenant Manager ausgelöst.

Der Failover-Prozess dauert in der Regel nur wenige Sekunden und ist schnell genug, dass Client-Applikationen nur geringe Auswirkungen haben und sich auf normale Wiederholungsmuster verlassen können, um den Betrieb fortzusetzen.

Wenn ein 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?

Es können HA-Gruppen (High Availability, Hochverfügbarkeit) verwendet werden, um hochverfügbare Verbindungen zu StorageGRID für Objektdaten und zur Verwendung durch den Administrator zur Verfügung zu stellen.

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

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

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

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

Zweck der HA-Gruppe	Fügen Sie diesem Typ Nodes der HA-Gruppe hinzu
S3-Client-Zugriff für "S3 Select"	<ul style="list-style-type: none"> • Service-Appliances • VMware-basierte Software-Nodes <p>Hinweis: HA-Gruppen werden bei der Verwendung von S3 Select empfohlen, aber nicht erforderlich.</p>

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

Wenn ein Grid Manager oder der Tenant Manager-Dienst ausfällt, wird das Failover von HA-Gruppen nicht ausgelöst.

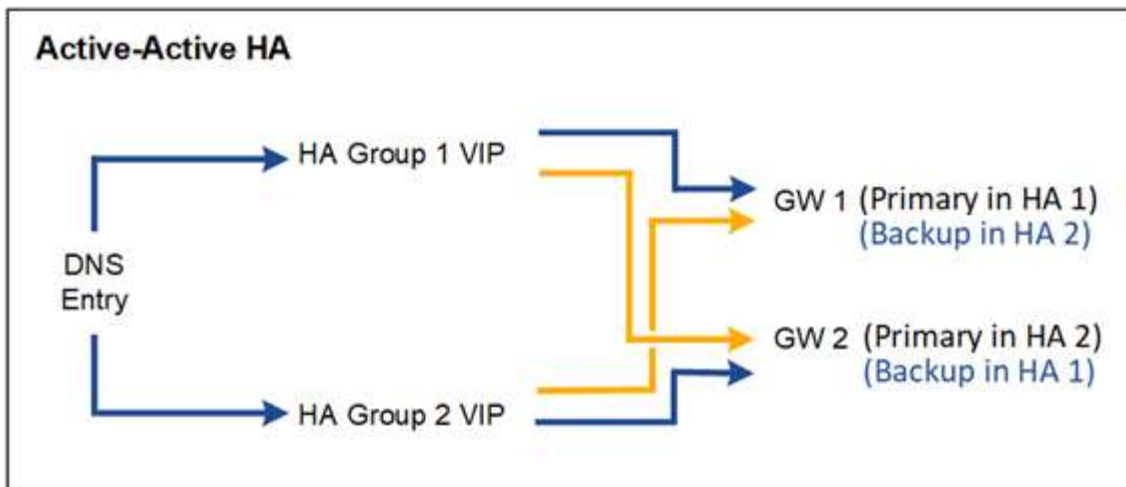
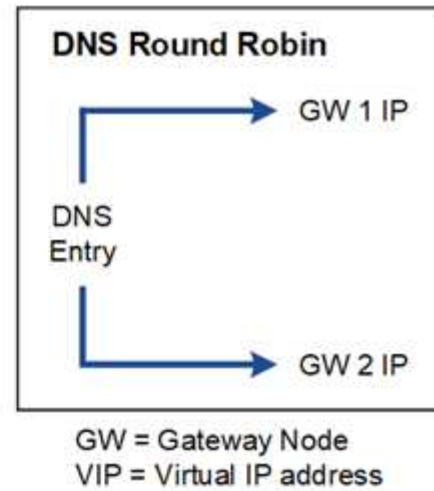
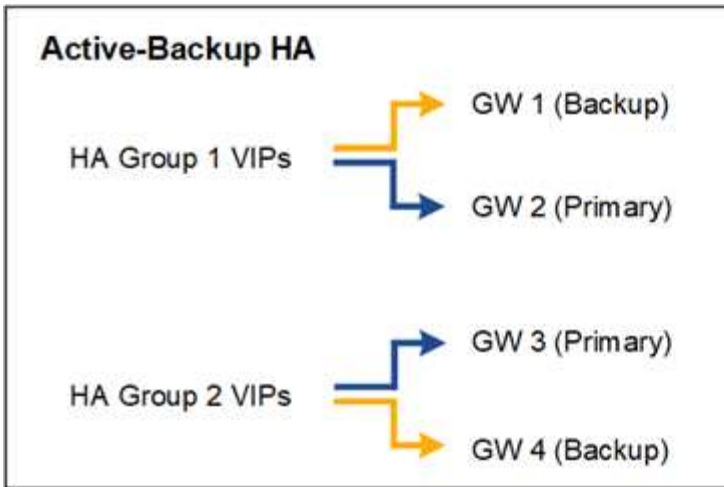
Wenn Sie sich bei einem Failover beim Grid Manager oder beim Tenant Manager angemeldet haben, werden Sie abgemeldet und müssen sich erneut anmelden, um Ihre Aufgabe fortzusetzen.

Einige Wartungsverfahren können nicht durchgeführt werden, wenn der primäre Admin-Node nicht verfügbar ist. Während des Failovers können Sie Ihr StorageGRID-System mit dem Grid-Manager 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 zeigt blau die primäre Schnittstelle in der HA-Gruppe an und gelb gibt die Backup-Schnittstelle in der HA-Gruppe an.



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

Konfiguration	Vorteile	Nachteile
Aktiv/Backup HA	<ul style="list-style-type: none"> Management über StorageGRID ohne externe Abhängigkeiten Schnelles Failover. 	<ul style="list-style-type: none"> In einer HA-Gruppe ist nur ein Node aktiv. Mindestens ein Node pro HA-Gruppe bleibt im Ruhezustand.
DNS Round Robin	<ul style="list-style-type: none"> Erhöhter Aggregatdurchsatz: Keine leerlaufenden Hosts 	<ul style="list-style-type: none"> Langsamer Failover, der vom Client-Verhalten abhängen kann. Konfiguration von Hardware außerhalb von StorageGRID erforderlich Benötigt eine vom Kunden implementierte Zustandsprüfung.

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

Konfigurieren Sie Hochverfügbarkeitsgruppen

Sie können Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen) konfigurieren, um hochverfügbaren Zugriff auf die Services in Admin-Nodes oder Gateway-Nodes bereitzustellen.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Root-Zugriffsberechtigung](#)".
- Wenn Sie eine VLAN-Schnittstelle in einer HA-Gruppe verwenden möchten, haben Sie die VLAN-Schnittstelle erstellt. Siehe "[Konfigurieren Sie die VLAN-Schnittstellen](#)".
- Wenn Sie eine Zugriffsoberfläche für einen Node in einer HA-Gruppe verwenden möchten, haben Sie die Schnittstelle erstellt:
 - **Red hat Enterprise Linux (vor der Installation des Knotens):** "[Erstellen von Node-Konfigurationsdateien](#)"
 - **Ubuntu oder Debian (vor der Installation des Knotens):** "[Erstellen von Node-Konfigurationsdateien](#)"
 - **Linux (nach der Installation des Knotens):** "[Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node](#)"
 - **VMware (nach der Installation des Knotens):** "[VMware: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node](#)"

Erstellen Sie eine Hochverfügbarkeitsgruppe

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

Eine Schnittstelle muss lauten, damit ein Gateway-Node oder ein Admin-Node in einer HA-Gruppe enthalten sein kann. Eine HA-Gruppe kann nur eine Schnittstelle für jeden angegebenen Node verwenden. Jedoch können andere Schnittstellen für denselben Node in anderen HA-Gruppen verwendet werden.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **CONFIGURATION > Network > High Availability groups**.
2. Wählen Sie **Erstellen**.

Geben Sie Details für die HA-Gruppe ein

Schritte

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

Fügen Sie der HA-Gruppe Schnittstellen hinzu

Schritte

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

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

Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.

Search... Total interface count: 4

Node	Interface	Site	IPv4 subnet	Node type
<input type="checkbox"/> DC1-ADM1-104-96	eth0	DC1	10.96.104.0/22	Primary Admin Node
<input type="checkbox"/> DC1-ADM1-104-96	eth2	DC1	—	Primary Admin Node
<input type="checkbox"/> DC2-ADM1-104-103	eth0	DC2	10.96.104.0/22	Admin Node
<input type="checkbox"/> DC2-ADM1-104-103	eth2	DC2	—	Admin Node

0 interfaces selected



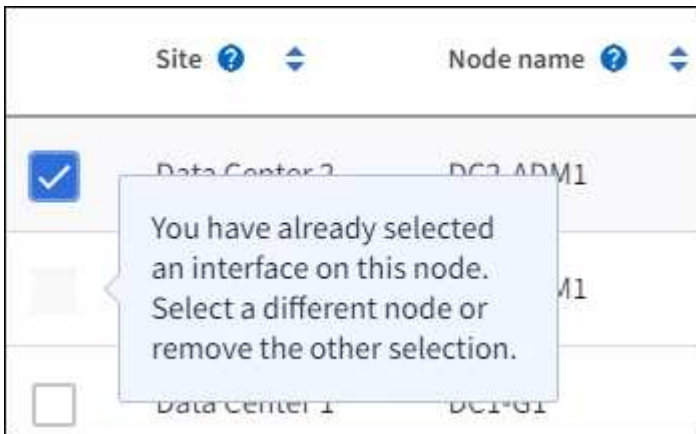
Warten Sie nach dem Erstellen einer VLAN-Schnittstelle bis zu 5 Minuten, bis die neue Schnittstelle in der Tabelle angezeigt wird.

Richtlinien für die Auswahl von Schnittstellen

- Sie müssen mindestens eine Schnittstelle auswählen.
- Sie können nur eine Schnittstelle für einen Node auswählen.
- Wenn die HA-Gruppe den HA-Schutz von Admin Node-Services bietet, zu denen der Grid Manager und der MandantenManager gehören, wählen Sie nur Schnittstellen zu Admin-Nodes aus.
- Wenn die HA-Gruppe für HA-Schutz für S3-Client-Datenverkehr geeignet ist, wählen Sie Schnittstellen auf Admin-Nodes, Gateway-Nodes oder beides aus.
- Wenn Sie Schnittstellen für verschiedene Node-Typen auswählen, wird ein Informationshinweis angezeigt. Sie werden daran erinnert, dass bei einem Failover Dienste, die vom zuvor aktiven Knoten bereitgestellt werden, möglicherweise auf dem neu aktiven Knoten nicht verfügbar sind. Ein Backup-Gateway-Node kann beispielsweise keinen HA-Schutz für Admin-Node-Services bereitstellen. Ebenso

kann ein Backup-Admin-Node nicht alle Wartungsverfahren durchführen, die der primäre Admin-Node bereitstellen kann.

- Wenn Sie keine Schnittstelle auswählen können, ist das Kontrollkästchen deaktiviert. Der QuickInfo enthält weitere Informationen.



- Eine Schnittstelle kann nicht ausgewählt werden, wenn ihr Subnetzwerk oder Gateway mit einer anderen ausgewählten Schnittstelle in Konflikt steht.
- Sie können keine konfigurierte Schnittstelle auswählen, wenn diese keine statische IP-Adresse hat.

2. Wählen Sie **Weiter**.

Legen Sie die Prioritätsreihenfolge fest

Wenn die HA-Gruppe mehr als eine Schnittstelle umfasst, können Sie feststellen, welche primäre Schnittstelle und welche Backup-Schnittstellen (Failover) sind. Wenn die primäre Schnittstelle fehlschlägt, werden die VIP-Adressen zur Schnittstelle mit der höchsten Priorität verschoben, die verfügbar ist. Wenn diese Schnittstelle ausfällt, werden die VIP-Adressen zur nächsten verfügbaren Schnittstelle mit der höchsten Priorität usw. verschoben.

Schritte

1. Ziehen Sie Zeilen in die Spalte **Priority order**, 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.

Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order	Node	Interface	Node type
1 (Primary interface)	DC1-ADM1-104-96	eth2	Primary Admin Node
2	DC2-ADM1-104-103	eth2	Admin Node



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

2. Wählen Sie **Weiter**.

Geben Sie die IP-Adressen ein

Schritte

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

Die Netzwerkadresse darf keine Host-Bits festgelegt haben. `192.16.0.0/22` Beispiel: .



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

Enter details for the HA group

Subnet CIDR

Specify the subnet in CIDR notation. The optional gateway IP and all VIPs must be in this subnet.

IPv4 address followed by a slash and the subnet length (0-32)

Gateway IP address (optional)

Optionally specify the IP address of the gateway, which must be in the subnet. If the subnet address length is 32, the gateway IP address is automatically set to the subnet IP.

Virtual IP address

Specify at least 1 and no more than 10 virtual IPs for the HA group. All virtual IPs must be in the same subnet. If the subnet length is 32, only one VIP is allowed, which is automatically set to the subnet/gateway IP.

[Add another IP address](#)

2. Wenn irgendwelche S3-Administrator- oder Mandanten-Clients von einem anderen Subnetz aus auf diese VIP-Adressen zugreifen, geben Sie optional die **Gateway-IP-Adresse** ein. Die Gateway-Adresse muss sich im VIP-Subnetz befinden.

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

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

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

4. Wählen Sie **HA-Gruppe erstellen** und wählen Sie **Fertig**.

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

Nächste Schritte

Wenn Sie diese HA-Gruppe zum Lastausgleich verwenden möchten, erstellen Sie einen Endpunkt zum Load Balancer, um den Port und das Netzwerkprotokoll zu ermitteln und die erforderlichen Zertifikate anzuschließen. Siehe "[Konfigurieren von Load Balancer-Endpunkten](#)".

Bearbeiten Sie eine Hochverfügbarkeitsgruppe

Sie können eine HA-Gruppe (High Availability, Hochverfügbarkeit) 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 Node, der einer ausgewählten Schnittstelle zugeordnet ist, entfernen möchten, wenn Sie ihn an einem Standort ausmustern oder einem Node entfernen möchten.

Schritte

1. Wählen Sie **CONFIGURATION > Network > High Availability groups**.

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 einen der folgenden Schritte aus, je nachdem, was Sie aktualisieren möchten:

- Wählen Sie **Aktionen > virtuelle IP-Adresse bearbeiten**, um VIP-Adressen hinzuzufügen oder zu entfernen.
- Wählen Sie **Aktionen > HA-Gruppe bearbeiten** aus, 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. Optional können Sie den Namen oder die Beschreibung der Gruppe aktualisieren.
- 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 am primären Admin-Node als primäre Schnittstelle auswählen. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden

- c. Optional können Sie Zeilen ziehen, um die Prioritätsreihenfolge der primären Schnittstelle und aller Backup-Schnittstellen für diese HA-Gruppe zu ändern.
- d. Optional können Sie die virtuellen IP-Adressen aktualisieren.

e. Wählen Sie **Speichern** und dann **Fertig stellen**.

Entfernen Sie eine Hochverfügbarkeitsgruppe

Sie können eine oder mehrere HA-Gruppen (High Availability, Hochverfügbarkeit) gleichzeitig entfernen.



Sie können eine HA-Gruppe nicht entfernen, wenn sie an einen Load Balancer-Endpunkt gebunden ist. Zum Löschen einer HA-Gruppe müssen Sie sie von allen Endpunkten der Load Balancer entfernen, die sie verwenden.

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

Schritte

1. Wählen Sie **CONFIGURATION > Network > High Availability groups**.
2. Überprüfen Sie die Spalte **Load Balancer Endpunkte** für jede HA-Gruppe, die Sie entfernen möchten. Wenn Load Balancer-Endpunkte aufgeführt sind:
 - a. Gehen Sie zu **CONFIGURATION > Network > 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 aufgeführt sind, aktivieren Sie das Kontrollkästchen für jede HA-Gruppe, die Sie entfernen möchten.
4. Wählen Sie **actions > Remove HA Group**.
5. Überprüfen Sie die Nachricht und wählen Sie **HA-Gruppe löschen**, um Ihre Auswahl zu bestätigen.

Alle von Ihnen ausgewählten HA-Gruppen werden entfernt. Ein grünes Banner wird auf der Seite „Hochverfügbarkeitsgruppen“ angezeigt.

Managen Sie den Lastausgleich

Überlegungen zum Lastausgleich

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

Was ist Load Balancing?

Wenn eine Client-Applikation Daten eines StorageGRID Systems speichert oder abrufen, verwendet StorageGRID einen Load Balancer, um den Aufnahme- und Abruf-Workload zu managen. Load Balancing maximiert die Geschwindigkeit und die Verbindungskapazität, indem der Workload auf mehrere Storage Nodes verteilt wird.

Der StorageGRID Load Balancer-Service wird auf allen Admin-Nodes und allen Gateway-Knoten installiert und bietet Layer 7-Lastausgleich. Sie beendet die TLS-Beendigung von Client-Anforderungen, prüft die

Anforderungen und stellt neue sichere Verbindungen zu den Storage-Nodes her.

Der Load Balancer-Service auf jedem Node wird unabhängig ausgeführt, wenn der Client-Datenverkehr an die Storage Nodes weitergeleitet wird. Durch eine Gewichtung leitet der Load Balancer-Service mehr Anfragen an Storage-Nodes mit höherer CPU-Verfügbarkeit weiter.



Obwohl der StorageGRID Load Balancer-Service der empfohlene Load-Balancing-Mechanismus ist, können Sie stattdessen einen Load Balancer eines Drittanbieters integrieren. Weitere Informationen erhalten Sie von Ihrem NetApp-Kundenbetreuer oder unter "[TR-4626: StorageGRID Anbieter- und Global Load Balancer](#)".

Wie viele Nodes für Lastausgleich benötige ich?

Als allgemeine Best Practice sollte jeder Standort in Ihrem StorageGRID-System zwei oder mehr Nodes mit dem Load Balancer Service umfassen. Ein Standort kann beispielsweise zwei Gateway-Nodes oder einen Admin-Node und einen Gateway-Node umfassen. Stellen Sie sicher, dass für jeden Load Balancing-Node eine geeignete Netzwerk-, Hardware- oder Virtualisierungsinfrastruktur bereitgestellt wird, unabhängig davon, ob Sie Services-Appliances, Bare-Metal-Nodes oder VM-basierte Nodes nutzen.

Was ist ein Endpunkt eines Load Balancers?

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

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

- "[Konfigurieren von Load Balancer-Endpunkten](#)"
- "[Verwenden Sie den S3-Einrichtungsassistenten](#)"
- "[Verwenden Sie den FabricPool-Einrichtungsassistenten](#)"

Überlegungen zum Port

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

Von anderen Netzdiensten verwendete Ports sind nicht zulässig. Siehe "[Referenz für Netzwerk-Ports](#)".

Überlegungen zum Netzwerkprotokoll

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

Überlegungen für Load Balancer-Endpointzertifikate

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

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

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

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

Welche Werte brauche ich?

Zum Erstellen des Zertifikats müssen Sie alle Domännennamen und IP-Adressen kennen, die S3-Client-Anwendungen für den Zugriff auf den Endpoint verwenden.

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

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

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

Wenn Sie virtuelle Anfragen im Hosted-Stil von S3 verwenden möchten, muss das Zertifikat für jeden konfigurierten Eintrag einen Eintrag **alternativer Name** enthalten ["Der Domänenname des S3-Endpunkts"](#), einschließlich aller Platzhalternamen. Beispiel:

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



Wenn Sie Platzhalter für Domännennamen verwenden, lesen Sie die ["Härtungsrichtlinien für Serverzertifikate"](#).

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

Wie verwalte ich auslaufende Zertifikate?



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

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

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

Überlegungen zum Bindungsmodus

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

Sie können einen der folgenden Bindungsmodi festlegen:

- **Global** (Standard): Client-Anwendungen können über die IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, die virtuelle IP-Adresse (VIP) einer HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie diese Einstellung, es sei denn, Sie müssen den Zugriff auf einen Endpunkt einschränken.
- **Virtuelle IPs von HA-Gruppen**. Client-Anwendungen müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden.
- **Knotenschnittstellen**. Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden.
- **Knotentyp**. Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden.

Überlegungen für den Mandantenzugriff

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

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



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

Beispiel für Mandantenzugriff

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

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

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

CPU-Verfügbarkeit

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

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

Konfigurieren von Load Balancer-Endpunkten

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



Swift-Details wurden aus dieser Version der doc-Site entfernt. Siehe ["Konfiguration von S3- und Swift-Client-Verbindungen"](#).

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die ["Root-Zugriffsberechtigung"](#).
- Sie haben die überprüft ["Überlegungen zum Lastausgleich"](#).
- Wenn Sie zuvor einen Port, den Sie für den Load Balancer-Endpunkt verwenden möchten, neu zugeordnet haben, haben Sie ["Port-Remap wurde entfernt"](#).

- Sie haben alle Hochverfügbarkeitsgruppen (High Availability groups, die Sie verwenden möchten, erstellt. HA-Gruppen werden empfohlen, jedoch nicht erforderlich. Siehe "[Management von Hochverfügbarkeitsgruppen](#)".
- Wenn der Load Balancer-Endpunkt verwendet wird "[S3 Mandanten für S3 Select](#)", darf er die IP-Adressen oder FQDNs von Bare-Metal-Knoten nicht verwenden. Für die für S3 Select verwendeten Load Balancer-Endpunkte sind nur Service-Appliances und VMware-basierte Software-Nodes zulässig.
- Sie haben alle VLAN-Schnittstellen konfiguriert, die Sie verwenden möchten. Siehe "[Konfigurieren Sie die VLAN-Schnittstellen](#)".
- Wenn Sie einen HTTPS-Endpunkt erstellen (empfohlen), haben Sie die Informationen für das Serverzertifikat.



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

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

Erstellen Sie einen Endpunkt für den Load Balancer

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

Greifen Sie auf den Assistenten zu

Schritte

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

Geben Sie Details zu Endpunkten ein

Schritte

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

S3- oder Swift-Client

Feld	Beschreibung
Name	Ein beschreibbarer Name für den Endpunkt, der in der Tabelle auf der Seite Load Balancer Endpunkte angezeigt wird.
Port	<p>Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist für den ersten erstellten Endpunkt standardmäßig auf 10433 eingestellt. Sie können jedoch jeden nicht verwendeten externen Port zwischen 1 und 65535 eingeben.</p> <p>Wenn Sie 80 oder 8443 eingeben, wird der Endpunkt nur auf Gateway Nodes konfiguriert, es sei denn, Sie haben Port 8443 freigegeben. Anschließend können Sie Port 8443 als S3-Endpunkt verwenden, und der Port wird sowohl auf dem Gateway als auch auf den Admin-Nodes konfiguriert.</p>
Client-Typ	Der Typ der Client-Anwendung, die diesen Endpunkt verwenden wird, entweder S3 oder Swift .
Netzwerkprotokoll	<p>Das Netzwerkprotokoll, das Clients bei der Verbindung mit diesem Endpunkt verwenden werden.</p> <ul style="list-style-type: none">• Wählen Sie HTTPS für sichere, TLS verschlüsselte Kommunikation (empfohlen). Sie müssen ein Sicherheitszertifikat anhängen, bevor Sie den Endpunkt speichern können.• Wählen Sie HTTP für eine weniger sichere, unverschlüsselte Kommunikation. Verwenden Sie HTTP nur für ein Grid, das nicht produktionsbereit ist.

Managementoberfläche

Feld	Beschreibung
Name	Ein beschreibbarer Name für den Endpunkt, der in der Tabelle auf der Seite Load Balancer Endpunkte angezeigt wird.
Port	<p>Der StorageGRID-Port, über den Sie auf den Grid-Manager, den Mandantenmanager oder beide zugreifen möchten.</p> <ul style="list-style-type: none">• Grid Manager: 8443• Mieter-Manager: 9443• Grid Manager und Tenant Manager: 443 <p>Hinweis: Sie können diese voreingestellten Ports oder andere verfügbare Ports verwenden.</p>
Schnittstellentyp	Aktivieren Sie das Optionsfeld für die StorageGRID-Schnittstelle, auf die Sie über diesen Endpunkt zugreifen möchten.

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

1. Wählen Sie **Weiter**.

Wählen Sie einen Bindungsmodus aus

Schritte

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

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

Modus	Beschreibung
Global (Standard für Client-Endpunkte)	<p>Clients können über die IP-Adresse eines beliebigen Gateway-Node oder Admin-Node, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen.</p> <p>Verwenden Sie die Einstellung Global, es sei denn, Sie müssen den Zugriff auf diesen Endpunkt einschränken.</p>
Virtuelle IPs von HA-Gruppen	<p>Clients müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen.</p> <p>Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überlappen.</p>
Node-Schnittstellen	<p>Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.</p>
Node-Typ (nur Client-Endpunkte)	<p>Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.</p>

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

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

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

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

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

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

Kontrolle des Mandantenzugriffs



Ein Endpunkt der Managementoberfläche kann den Mandantenzugriff nur steuern, wenn der Endpunkt über den verfügt [Schnittstellentyp des Tenant Manager](#).

Schritte

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

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen. Sie müssen diese Option auswählen, wenn Sie noch keine Mandantenkonten erstellt haben. Nachdem Sie Mandantenkonten hinzugefügt haben, können Sie den Load Balancer-Endpunkt bearbeiten, um bestimmte Konten zuzulassen oder zu blockieren.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt für den Zugriff auf ihre Buckets verwenden.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Dieser Endpunkt kann von allen anderen Mandanten verwendet werden.

2. Wenn Sie einen **HTTP**-Endpunkt erstellen, müssen Sie kein Zertifikat anhängen. Wählen Sie **Erstellen**, um den neuen Load Balancer-Endpunkt hinzuzufügen. Dann gehen Sie zu [Nachdem Sie fertig sind](#).

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

Zertifikat anhängen

Schritte

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

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

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

Sie können diese Option nur auswählen, wenn Sie das von der Grid-CA signierte Standard-S3-API-Zertifikat durch ein benutzerdefiniertes Zertifikat ersetzt haben, das von einer externen Zertifizierungsstelle signiert wurde. Siehe "[Konfigurieren Sie S3-API-Zertifikate](#)".

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

Zertifikat hochladen

- a. Wählen Sie **Zertifikat hochladen**.
- b. Laden Sie die erforderlichen Serverzertifikatdateien hoch:
 - **Server-Zertifikat:** Die benutzerdefinierte Server-Zertifikatdatei in PEM-Kodierung.
 - **Zertifikat privater Schlüssel:** Die benutzerdefinierte Server Zertifikat private Schlüsseldatei (.key).



EC Private Keys müssen mindestens 224 Bit groß sein. RSA Private Keys müssen mindestens 2048 Bit groß sein.

- **CA-Paket:** Eine einzelne optionale Datei, die die Zertifikate jeder Intermediate-Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.
- c. Erweitern Sie **Zertifikatdetails**, um die Metadaten für jedes hochgeladene Zertifikat anzuzeigen. Wenn Sie ein optionales CA-Paket hochgeladen haben, wird jedes Zertifikat auf seiner eigenen Registerkarte angezeigt.
 - Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern, oder wählen Sie **CA-Paket herunterladen**, um das Zertifikatspaket zu speichern.

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

Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat kopieren PEM** oder **CA-Paket kopieren PEM** aus, um den Zertifikatsinhalt zum Einfügen an eine andere Stelle zu kopieren.
- d. Wählen Sie **Erstellen**. + der Endpunkt des Load Balancer wird erstellt. Das benutzerdefinierte Zertifikat wird für alle nachfolgenden neuen Verbindungen zwischen S3-Clients oder der Managementoberfläche und dem Endpunkt verwendet.

Zertifikat wird generiert

- a. Wählen Sie **Zertifikat erstellen**.
- b. Geben Sie die Zertifikatsinformationen an:

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

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

c. Wählen Sie **Erzeugen**.

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

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

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

Beispiel: `storagegrid_certificate.pem`

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

e. Wählen Sie **Erstellen**.

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

Nachdem Sie fertig sind

Schritte

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

Die IP-Adresse, die Sie im DNS-Datensatz eingeben, hängt davon ab, ob Sie eine HA-Gruppe von Load-Balancing-Nodes verwenden:

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

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

2. Bereitstellen der für die Verbindung mit dem Endpunkt erforderlichen Informationen für S3-Clients:

- Port-Nummer
- Vollständig qualifizierter Domain-Name oder IP-Adresse
- Alle erforderlichen Zertifikatsdetails

Load Balancer-Endpunkte anzeigen und bearbeiten

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

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

S3 load balancer endpoint

Port:	10443
Client type:	S3
Network protocol:	HTTPS
Binding mode:	Global
Endpoint ID:	3d02c126-9437-478c-8b24-08384401d3cb

Remove

Binding mode
Certificate
Tenant access (2 allowed)

You can select a different binding mode or change IP addresses for the current binding mode.

Edit binding mode

Binding mode: Global

This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.

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



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



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

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

Aufgabe	Menü „Aktionen“	Detailseite
Endpunktzertifikat bearbeiten	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie Aktionen > Endpunktzertifikat bearbeiten aus. c. Laden Sie nach Bedarf ein neues benutzerdefiniertes Zertifikat hoch oder generieren Sie es oder beginnen Sie mit der Verwendung des globalen S3-Zertifikats. d. Wählen Sie Änderungen speichern. 	<ul style="list-style-type: none"> a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Zertifikat aus. c. Wählen Sie Zertifikat bearbeiten. d. Laden Sie nach Bedarf ein neues benutzerdefiniertes Zertifikat hoch oder generieren Sie es oder beginnen Sie mit der Verwendung des globalen S3-Zertifikats. e. Wählen Sie Änderungen speichern.
Bearbeiten Sie den Mandantenzugriff	<ul style="list-style-type: none"> a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie actions > Edit Tenant Access. c. Wählen Sie eine andere Zugriffsoption aus, wählen Sie Mandanten aus der Liste aus oder entfernen Sie sie aus oder führen Sie beides aus. d. Wählen Sie Änderungen speichern. 	<ul style="list-style-type: none"> a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Tenant Access. c. Wählen Sie Mandantenzugriff bearbeiten. d. Wählen Sie eine andere Zugriffsoption aus, wählen Sie Mandanten aus der Liste aus oder entfernen Sie sie aus oder führen Sie beides aus. e. Wählen Sie Änderungen speichern.

Entfernen Sie Load Balancer-Endpunkte

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



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



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

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

- a. Wählen Sie auf der Seite Load Balancer den Endpunktnamen aus.
- b. Wählen Sie auf der Detailseite * Entfernen.
- c. Wählen Sie **OK**.

Konfigurieren Sie die Domännennamen des S3-Endpunkts

Um Anforderungen im virtuellen Hosted-Stil von S3 zu unterstützen, müssen Sie die Liste der S3-Endpunkt-Domännennamen, mit denen S3-Clients eine Verbindung herstellen, mit dem Grid Manager konfigurieren.



Die Verwendung einer IP-Adresse für einen Domännennamen des Endpunkts wird nicht unterstützt. Zukünftige Versionen verhindern diese Konfiguration.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben "[Bestimmte Zugriffsberechtigungen](#)".
- Sie haben bestätigt, dass ein Grid-Upgrade nicht ausgeführt wird.



Nehmen Sie keine Änderungen an der Domännennamenkonfiguration vor, wenn ein Grid-Upgrade durchgeführt wird.

Über diese Aufgabe

Um Clients die Verwendung von S3-Endpunkt-Domain-Namen zu ermöglichen, müssen Sie folgende Aktionen durchführen:

- Verwenden Sie den Grid-Manager, um dem StorageGRID System die S3-Endpunkt-Domain-Namen hinzuzufügen.
- Stellen Sie sicher, dass der "[Zertifikat, das der Client für HTTPS-Verbindungen zu StorageGRID verwendet](#)" für alle vom Client benötigten Domännennamen signiert ist.

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

- Konfigurieren Sie den vom Client verwendeten DNS-Server. Fügen Sie DNS-Datensätze für die IP-Adressen ein, die Clients zum Verbindungsaufbau verwenden, und stellen Sie sicher, dass die Datensätze auf alle erforderlichen S3-Endpunkt-Domännennamen verweisen, einschließlich aller Platzhalternamen.



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

Clients, die HTTPS-Verbindungen (empfohlen) zum Raster verwenden, können eines der folgenden 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-Endpunkt-Domännennamen erkennt.

- Clients, die sich mit einem Load-Balancer-Endpunkt oder direkt mit einem Storage-Node verbinden, können das globale S3-API-Zertifikat so anpassen, dass alle erforderlichen S3-Endpunkt-Domännennamen berücksichtigt werden.



Wenn Sie keine S3-Endpunkt-Domännennamen hinzufügen und die Liste leer ist, wird die Unterstützung für Anforderungen im virtuellen Hosted-Stil von S3 deaktiviert.

Fügen Sie einen S3-Endpunkt-Domännennamen hinzu

Schritte

1. Wählen Sie **CONFIGURATION > Network > S3-Endpunkt-Domännennamen**.
2. Geben Sie den Domainnamen in das Feld **Domain Name 1** ein. Wählen Sie **Add another Domain Name**, um weitere Domainnamen hinzuzufügen.
3. Wählen Sie **Speichern**.
4. Stellen Sie sicher, dass die von Clients verwendeten Serverzertifikate mit den erforderlichen S3-Endpunkt-Domännennamen 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 oder direkt zu Storage Nodes verwendet, "[Aktualisieren Sie das globale S3-API-Zertifikat](#)".
5. Fügen Sie die erforderlichen DNS-Einträge hinzu, um sicherzustellen, dass die Anforderungen für den Domännennamen des Endpunkts aufgelöst werden können.

Ergebnis

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

Benennen Sie einen S3-Endpunkt-Domännennamen um

Wenn Sie einen Namen ändern, der von S3-Anwendungen verwendet wird, schlagen Anforderungen im virtuellen Hosted-Stil fehl.


Schritte

1. Wählen Sie **CONFIGURATION > Network > S3-Endpunkt-Domännennamen**.
2. Wählen Sie das Feld für den Domännennamen 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 Sie einen S3-Endpunkt-Domännennamen

Wenn Sie einen Namen entfernen, der von S3-Anwendungen verwendet wird, schlagen Anforderungen im virtuellen Hosted-Stil fehl.

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **S3-Endpunkt-Domännennamen**.
2. Wählen Sie das Löschsymbolsymbol  neben dem Domännennamen aus.
3. Wählen Sie **Ja**, um den Löschvorgang zu bestätigen.

Verwandte Informationen

- ["S3-REST-API VERWENDEN"](#)
- ["Zeigen Sie IP-Adressen an"](#)
- ["Konfigurieren Sie Hochverfügbarkeitsgruppen"](#)

Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen

Zum Speichern oder Abrufen von Objekten 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 Storage-Nodes enthalten ist.

Client-Applikationen können mithilfe der IP-Adresse eines Grid-Node und der Portnummer des Service auf diesem Node eine Verbindung zu StorageGRID herstellen. Optional können Sie Gruppen für Hochverfügbarkeit (High Availability, HA) von Load-Balancing-Nodes erstellen, um hochverfügbare Verbindungen bereitzustellen, die virtuelle IP-Adressen (VIP) verwenden. Wenn Sie eine Verbindung zu StorageGRID über einen vollständig qualifizierten Domännennamen (FQDN) anstelle einer IP- oder VIP-Adresse herstellen möchten, können Sie DNS-Einträge konfigurieren.

In dieser Tabelle sind die verschiedenen Verbindungsmethoden aufgeführt, mit denen Clients eine Verbindung zu StorageGRID herstellen können, sowie die für den jeweiligen Verbindungstyp verwendeten IP-Adressen und Ports. Wenn Sie bereits Load Balancer-Endpunkte und HA-Gruppen (Hochverfügbarkeitsgruppen) erstellt haben, finden Sie unter [Wo finden Sie IP-Adressen](#) diese Werte im Grid Manager.

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
HA-Gruppe	Lastausgleich	Virtuelle IP-Adresse einer HA-Gruppe	Port, der dem Endpunkt des Lastausgleichs zugewiesen ist
Admin-Node	Lastausgleich	IP-Adresse des Admin-Knotens	Port, der dem Endpunkt des Lastausgleichs zugewiesen ist
Gateway-Node	Lastausgleich	IP-Adresse des Gateway-Node	Port, der dem Endpunkt des Lastausgleichs zugewiesen ist
Storage-Node	LDR	IP-Adresse des Speicherknoten	S3-Standard-Ports: <ul style="list-style-type: none"> • HTTPS: 18082 • HTTP: 18084

Beispiel-URLs

Um eine Client-Applikation mit dem Endpunkt Load Balancer einer HA-Gruppe von Gateway Nodes zu verbinden, verwenden Sie eine wie unten gezeigt strukturierte URL:

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

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

```
https://192.0.2.5:10443
```

Wo finden Sie IP-Adressen

1. Melden Sie sich mit einem beim Grid-Manager an "[Unterstützter Webbrowser](#)".
2. So suchen Sie die IP-Adresse eines Grid-Knotens:
 - a. Wählen Sie **KNOTEN**.
 - b. Wählen Sie den Admin-Node, Gateway-Node oder Storage-Node aus, mit dem Sie eine Verbindung herstellen möchten.
 - c. Wählen Sie die Registerkarte **Übersicht**.
 - d. Notieren Sie im Abschnitt Node-Informationen die IP-Adressen für den Node.
 - e. Wählen Sie **Mehr anzeigen**, um IPv6-Adressen und Schnittstellen-Zuordnungen anzuzeigen.

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

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



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

3. So finden Sie die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe:
 - a. Wählen Sie **CONFIGURATION > Network > High Availability groups**.
 - 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 **CONFIGURATION > Network > Load Balancer Endpunkte**.
 - b. Notieren Sie sich die Portnummer für den zu verwendenden Endpunkt.



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

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

- d. Bestätigen Sie, dass der **Client-Typ** (S3) mit der Client-Anwendung übereinstimmt, die den Endpunkt verwendet.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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