# Verwalten von StorageGRID-Netzwerken und -Verbindungen

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/de-de/storagegrid-115/admin/guidelines-for-storagegrid-networks.html on October 03, 2025. Always check docs.netapp.com for the latest.

# Inhalt

# Verwalten von StorageGRID-Netzwerken und -Verbindungen

Mit dem Grid Manager können Sie StorageGRID-Netzwerke und -Verbindungen konfigurieren und verwalten.

Siehe "Konfigurieren von S3- und Swift-Client-Verbindungen" Informationen zum Verbinden von S3 oder Swift Clients

- "Richtlinien für StorageGRID-Netzwerke"
- "Anzeigen von IP-Adressen"
- "Unterstützte Chiffren für ausgehende TLS-Verbindungen"
- "Die Netzwerkübertragungsverschlüsselung wird geändert"
- "Serverzertifikate werden konfiguriert"
- "Konfigurieren von Speicher-Proxy-Einstellungen"
- "Konfigurieren von Administrator-Proxy-Einstellungen"
- "Verwalten von Richtlinien für die Verkehrsklassifizierung"
- "Was sind Verbindungskosten"

# Richtlinien für StorageGRID-Netzwerke

StorageGRID unterstützt bis zu drei Netzwerkschnittstellen pro Grid Node. So können Sie das Netzwerk für jeden einzelnen Grid Node so konfigurieren, dass die Sicherheits- und Zugriffsanforderungen erfüllt werden.

Informationen zum Ändern oder Hinzufügen eines Netzwerks für einen Grid-Node finden Sie in den Recovery- und Wartungsanweisungen. Weitere Informationen zur Netzwerktopologie finden Sie in den Netzwerkanweisungen.

## Grid-Netzwerk

Erforderlich. Das Grid-Netzwerk wird für den gesamten internen StorageGRID-Datenverkehr verwendet. Das System bietet Konnektivität zwischen allen Nodes im Grid und allen Standorten und Subnetzen.

## Admin-Netzwerk

Optional Das Admin-Netzwerk wird in der Regel für die Systemadministration und -Wartung verwendet. Sie kann auch für den Zugriff auf das Client-Protokoll verwendet werden. Das Admin-Netzwerk ist in der Regel ein privates Netzwerk und muss nicht zwischen Standorten routingfähig sein.

## Client-Netzwerk

Optional Das Client-Netzwerk ist ein offenes Netzwerk, das normalerweise für den Zugriff auf S3- und Swift-Client-Applikationen verwendet wird, sodass das Grid-Netzwerk isoliert und gesichert werden kann. Das Client-Netzwerk kann mit jedem Subnetz kommunizieren, das über das lokale Gateway erreichbar ist.

## Richtlinien

- Jeder StorageGRID Grid Node benötigt für jedes ihm zugewiesene Netzwerk eine dedizierte Netzwerkschnittstelle, eine IP-Adresse, eine Subnetzmaske und ein Gateway.
- Ein Grid-Node kann nicht mehr als eine Schnittstelle in einem Netzwerk haben.
- Es wird ein einzelnes Gateway pro Netzwerk und pro Grid-Node unterstützt, das sich im gleichen Subnetz wie der Node befindet. Sie können bei Bedarf komplexere Routing-Lösungen im Gateway implementieren.
- Auf jedem Node ist jedes Netzwerk einer bestimmten Netzwerkschnittstelle zugeordnet.

| Netzwerk | Schnittstellenname |
|---|---|
| Raster | Eth0 |
| Admin (optional) | Eth1 |
| Client (optional) | Eth2 |

- Wenn der Node mit einer StorageGRID Appliance verbunden ist, werden für jedes Netzwerk bestimmte Ports verwendet. Weitere Informationen finden Sie in den Installationsanweisungen für Ihr Gerät.
- Die Standardroute wird automatisch pro Knoten generiert. Wenn eth2 aktiviert ist, verwendet 0.0.0.0/0 das Client-Netzwerk auf eth2. Wenn eth2 nicht aktiviert ist, verwendet 0.0.0.0/0 das Grid-Netzwerk auf eth0.
- Das Client-Netzwerk ist erst betriebsbereit, wenn der Grid-Node dem Grid beigetreten ist
- Das Admin-Netzwerk kann während der Bereitstellung des Grid-Knotens konfiguriert werden, um den Zugriff auf die Installations-Benutzeroberfläche zu ermöglichen, bevor das Grid vollständig installiert ist.

**Verwandte Informationen**

"Verwalten Sie erholen"

"Netzwerkrichtlinien"

# Anzeigen von IP-Adressen

Sie können die IP-Adresse für jeden Grid-Node im StorageGRID System anzeigen. Sie können diese IP-Adresse dann verwenden, um sich bei dem Grid-Node über die Befehlszeile anzumelden und verschiedene Wartungsvorgänge auszuführen.

**Was Sie benötigen**

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

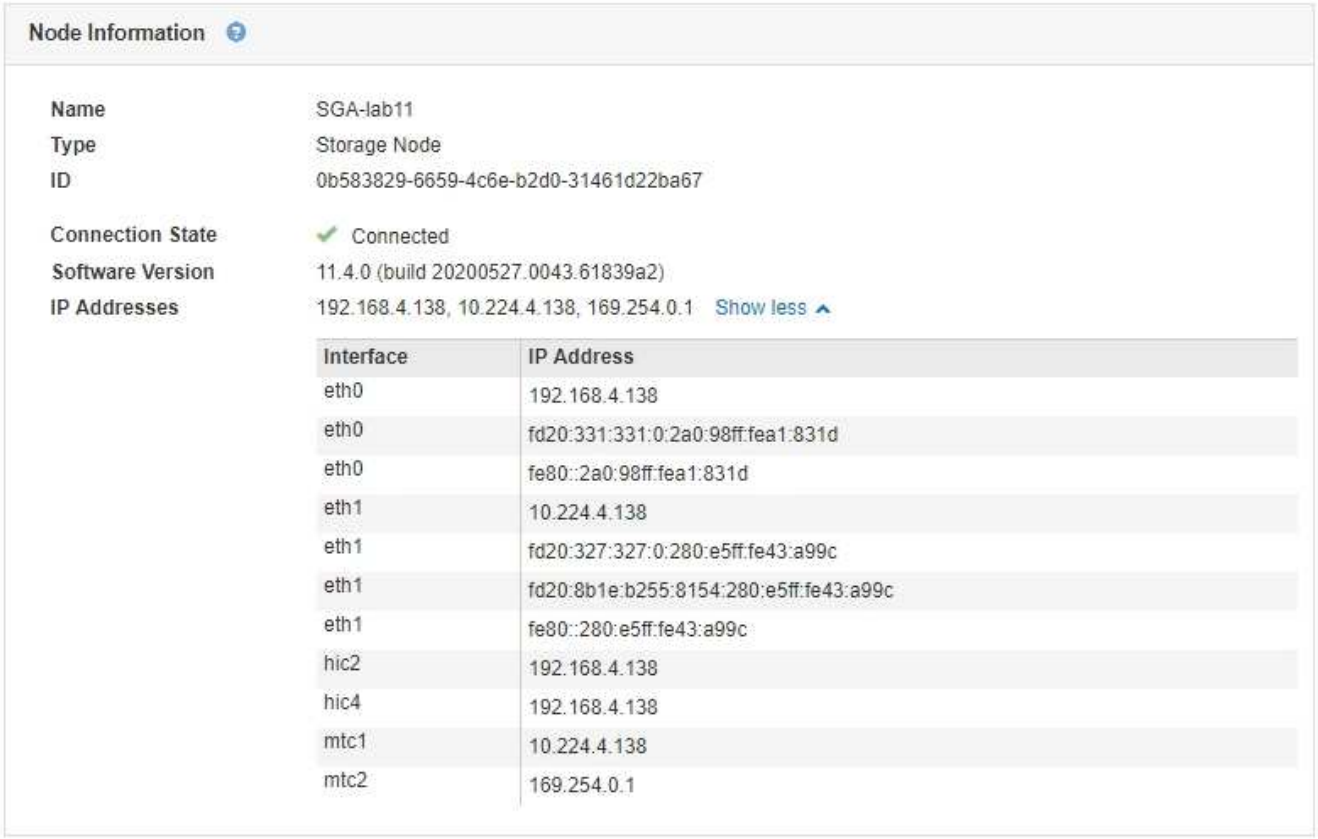
**Über diese Aufgabe**

Informationen zum Ändern von IP-Adressen finden Sie in den Wiederherstellungsanleitungen und Wartungsanweisungen.

**Schritte**

1. Wählen Sie **Nodes** > ***Grid Node*** > **Übersicht**.
2. Klicken Sie rechts neben dem Titel der IP-Adressen auf **Mehr anzeigen**.

   Die IP-Adressen für diesen Grid-Node werden in einer Tabelle aufgeführt.




**Verwandte Informationen**

"Verwalten Sie erholen"

# Unterstützte Chiffren für ausgehende TLS-Verbindungen

Das StorageGRID System unterstützt eine begrenzte Anzahl von Verschlüsselungssuiten für TLS-Verbindungen (Transport Layer Security) zu den externen Systemen, die für Identitätsföderation und Cloud-Storage-Pools verwendet werden.

## Unterstützte Versionen von TLS

StorageGRID unterstützt TLS 1.2 und TLS 1.3 für Verbindungen zu externen Systemen, die für Identitätsföderation und Cloud-Storage-Pools verwendet werden.

Die zur Verwendung mit externen Systemen unterstützten TLS-Chiffren wurden ausgewählt, um die Kompatibilität mit verschiedenen externen Systemen sicherzustellen. Die Liste ist größer als die Liste der Chiffren, die zur Verwendung mit S3- oder Swift-Client-Applikationen unterstützt werden.

> TLS-Konfigurationsoptionen wie Protokollversionen, Chiffren, Schlüsselaustausch-Algorithmen und MAC-Algorithmen sind in StorageGRID nicht konfigurierbar. Wenden Sie sich an Ihren NetApp Ansprechpartner, wenn Sie spezifische Anfragen zu diesen Einstellungen haben.

## Unterstützte TLS 1.2-Cipher-Suiten

Die folgenden TLS 1.2-Chiffre-Suiten werden unterstützt:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

### Unterstützte TLS 1.3-Cipher-Suiten

Die folgenden TLS 1.3-Chiffre-Suiten werden unterstützt:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

# Die Netzwerkübertragungsverschlüsselung wird geändert

Das StorageGRID System verwendet Transport Layer Security (TLS) zum Schutz des internen Kontrolldatenverkehrs zwischen den Grid-Nodes. Die Option „Netzwerkübertragungsverschlüsselung“ legt den von TLS verwendeten Algorithmus zur Verschlüsselung der Datenverkehrskontrolle zwischen den Grid-Nodes fest. Diese Einstellung hat keine Auswirkung auf die Datenverschlüsselung.

**Was Sie benötigen**

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

**Über diese Aufgabe**

Standardmäßig verwendet die Netzwerkübertragungsverschlüsselung den AES256-SHA-Algorithmus. Der Kontrolldatenverkehr kann auch mit dem AES128-SHA-Algorithmus verschlüsselt werden.

**Schritte**

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Gitteroptionen**.
2. Ändern Sie im Abschnitt Netzwerkoptionen die Netzwerkübertragungsverschlüsselung in **AES128-SHA** oder **AES256-SHA** (Standardeinstellung).

3. Klicken Sie Auf **Speichern**.

# Serverzertifikate werden konfiguriert

Sie können die vom StorageGRID-System verwendeten Serverzertifikate anpassen.

Das StorageGRID System verwendet Sicherheitszertifikate für mehrere unterschiedliche Zwecke:

- Management Interface Server Certificates: Dient zum sicheren Zugriff auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API.
- Storage API Server Certificates: Dient zum sicheren Zugriff auf die Storage Nodes und Gateway Nodes, welche API-Client-Anwendungen zum Hochladen und Herunterladen von Objektdaten verwenden.

Sie können die während der Installation erstellten Standardzertifikate verwenden oder diese Standardtypen durch Ihre eigenen benutzerdefinierten Zertifikate ersetzen.

## Unterstützte Arten von benutzerdefiniertem Serverzertifikat

Das StorageGRID-System unterstützt benutzerdefinierte Serverzertifikate, die mit RSA oder ECDSA (Algorithmus für digitale Signaturen der Elliptischen Kurve) verschlüsselt sind.

Weitere Informationen dazu, wie StorageGRID Client-Verbindungen für DIE REST-API sichert, finden Sie in den S3 oder Swift-Implementierungsleitfäden.

## Zertifikate für Load Balancer-Endpunkte

StorageGRID managt die für Load Balancer-Endpunkte verwendeten Zertifikate separat. Informationen zum Konfigurieren von Load Balancer-Zertifikaten finden Sie in den Anweisungen zum Konfigurieren von Load Balancer-Endpunkten.

**Verwandte Informationen**

"S3 verwenden"

"Verwenden Sie Swift"

"Konfigurieren von Load Balancer-Endpunkten"

## Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager

Sie können das standardmäßige StorageGRID-Serverzertifikat durch ein einzelnes benutzerdefiniertes Serverzertifikat ersetzen, das Benutzern den Zugriff auf den Grid-Manager und den Tenant-Manager ermöglicht, ohne dass Sicherheitswarnungen ausgegeben werden.

**Über diese Aufgabe**

Standardmäßig wird jeder Admin-Node ein von der Grid-CA signiertes Zertifikat ausgestellt. Diese CA-signierten Zertifikate können durch ein einziges allgemeines benutzerdefiniertes Serverzertifikat und den entsprechenden privaten Schlüssel ersetzt werden.

Da ein einzelnes benutzerdefiniertes Serverzertifikat für alle Administratorknoten verwendet wird, müssen Sie

das Zertifikat als Platzhalter- oder Multi-Domain-Zertifikat angeben, wenn Clients bei der Verbindung mit Grid Manager und Tenant Manager den Hostnamen überprüfen müssen. Definieren Sie das benutzerdefinierte Zertifikat so, dass es mit allen Admin-Nodes im Raster übereinstimmt.

Sie müssen die Konfiguration auf dem Server abschließen, und je nach der von Ihnen verwendeten Root Certificate Authority (CA) müssen Benutzer möglicherweise auch das Root CA-Zertifikat im Webbrowser installieren, mit dem sie auf den Grid Manager und den Tenant Manager zugreifen.

> Um sicherzustellen, dass die Vorgänge nicht durch ein Serverzertifikat unterbrochen werden, werden die Warnung **Ablauf des Serverzertifikats für die Managementoberfläche** und der Alarm Legacy Management Interface Certificate Expiry (MCEP) ausgelöst, wenn dieses Serverzertifikat abläuft. Nach Bedarf können Sie die Anzahl der Tage anzeigen, bis das aktuelle Service-Zertifikat abläuft, indem Sie **Support** > **Tools** > **Grid Topology** auswählen. Wählen Sie dann ***primary Admin Node*** > **CMN** > **Ressourcen** aus.

> Wenn Sie mit einem Domänennamen anstelle einer IP-Adresse auf den Grid Manager oder den Tenant Manager zugreifen, zeigt der Browser einen Zertifikatfehler ohne eine Option zum Umgehen an, wenn eine der folgenden Fälle auftritt:
>
> - Ihr Zertifikat für den benutzerdefinierten Verwaltungsserver läuft ab.
> - Sie werden von einem Server-Zertifikat der benutzerdefinierten Managementoberfläche auf das Standardserverzertifikat zurückgesetzt.

**Schritte**

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Klicken Sie im Abschnitt Management Interface Server Certificate auf **Benutzerdefiniertes Zertifikat installieren**.
3. Laden Sie die erforderlichen Serverzertifikatdateien hoch:
   - **Server-Zertifikat**: Die benutzerdefinierte Server-Zertifikatdatei (`.crt`).
   - **Server Certificate Private Key**: Die benutzerdefinierte Server Zertifikat private Schlüssel Datei (`.key`).

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

   - **CA Bundle**: Eine einzelne Datei, die die Zertifikate jeder Intermediate Emission Certificate Authority (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.
4. Klicken Sie Auf **Speichern**.

   Die benutzerdefinierten Serverzertifikate werden für alle nachfolgenden neuen Clientverbindungen verwendet.

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

   > Nachdem Sie ein neues Zertifikat hochgeladen haben, lassen Sie bis zu einem Tag, bis alle zugehörigen Alarme zum Ablauf des Zertifikats (oder ältere Alarme) gelöscht werden können.

5. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

## Wiederherstellen der Standard-Serverzertifikate für den Grid Manager und den Tenant Manager

Sie können auf die Verwendung der Standard-Serverzertifikate für den Grid Manager und den Tenant Manager zurücksetzen.

**Schritte**

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Klicken Sie im Abschnitt Schnittstellenserverzertifikat verwalten auf **Standardzertifikate verwenden**.
3. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

   Wenn Sie die Standardserverzertifikate wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Die Standard-Serverzertifikate werden für alle nachfolgenden neuen Clientverbindungen verwendet.

4. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

## Konfigurieren eines benutzerdefinierten Serverzertifikats für Verbindungen mit dem Speicherknoten oder dem CLB-Dienst

Sie können das Serverzertifikat, das für S3- oder Swift-Client-Verbindungen zum Storage-Node oder zum CLB-Service (veraltet) auf Gateway-Node verwendet wird, ersetzen. Das benutzerdefinierte Ersatzserverzertifikat ist speziell für Ihr Unternehmen bestimmt.

**Über diese Aufgabe**

Standardmäßig wird jeder Speicherknoten ein X.509-Serverzertifikat ausgestellt, das von der Grid-CA signiert wurde. Diese CA-signierten Zertifikate können durch ein einziges allgemeines benutzerdefiniertes Serverzertifikat und den entsprechenden privaten Schlüssel ersetzt werden.

Für alle Speicherknoten wird ein einzelnes benutzerdefiniertes Serverzertifikat verwendet. Sie müssen daher das Zertifikat als Platzhalter- oder Multidomain-Zertifikat angeben, wenn Clients den Hostnamen bei der Verbindung mit dem Speicherendpunkt überprüfen müssen. Definieren Sie das benutzerdefinierte Zertifikat, sodass es mit allen Speicherknoten im Raster übereinstimmt.

Nach Abschluss der Konfiguration auf dem Server müssen Benutzer möglicherweise auch das Root-CA-Zertifikat im S3- oder Swift-API-Client installieren, den sie für den Zugriff auf das System verwenden, abhängig von der Root Certificate Authority (CA), die Sie verwenden.

> Um sicherzustellen, dass die Vorgänge nicht durch ein ausgefallenes Serverzertifikat unterbrochen werden, wird der Alarm **Ablauf des Serverzertifikats für Storage API Endpunkte** und der Alarm Legacy Storage API Service Endpoints Certificate Expiry (SCEP) ausgelöst, wenn das Root-Server-Zertifikat abläuft. Nach Bedarf können Sie die Anzahl der Tage anzeigen, bis das aktuelle Service-Zertifikat abläuft, indem Sie **Support** > **Tools** > **Grid Topology** auswählen. Wählen Sie dann ***primary Admin Node*** > **CMN** > **Ressourcen** aus.

Die benutzerdefinierten Zertifikate werden nur verwendet, wenn Clients über den veralteten CLB-Dienst auf Gateway-Nodes eine Verbindung zu StorageGRID herstellen oder eine direkte Verbindung zu Storage-Nodes

herstellen. S3- oder Swift-Clients, die über den Load Balancer Service am Admin-Nodes oder Gateway-Nodes eine Verbindung zu StorageGRID herstellen, verwenden das für den Load Balancer-Endpunkt konfigurierte Zertifikat.

> Die Warnung **Ablauf des Load Balancer-Endpunktzertifikats** wird für Load Balancer-Endpunkte ausgelöst, die bald ablaufen.

**Schritte**

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Klicken Sie im Abschnitt Serverzertifikat für Objekt-Storage-API-Service-Endpunkte auf **Benutzerdefiniertes Zertifikat installieren**.
3. Laden Sie die erforderlichen Serverzertifikatdateien hoch:
   - **Server-Zertifikat**: Die benutzerdefinierte Server-Zertifikatdatei (`.crt`).
   - **Server Certificate Private Key**: Die benutzerdefinierte Server Zertifikat private Schlüssel Datei (`.key`).

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

   - **CA Bundle**: Eine einzelne Datei, die die Zertifikate jeder Intermediate Emission Certificate Authority (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.
4. Klicken Sie Auf **Speichern**.

   Das benutzerdefinierte Serverzertifikat wird für alle nachfolgenden neuen API-Client-Verbindungen verwendet.

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

   > Nachdem Sie ein neues Zertifikat hochgeladen haben, lassen Sie bis zu einem Tag, bis alle zugehörigen Alarme zum Ablauf des Zertifikats (oder ältere Alarme) gelöscht werden können.

5. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

**Verwandte Informationen**

"S3 verwenden"

"Verwenden Sie Swift"

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

## Wiederherstellen der Standard-Serverzertifikate für die S3- und Swift-REST-API-Endpunkte

Sie können die Standardeinstellungen für die S3- und Swift-REST-API-Endpunkte verwenden.

**Schritte**

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Klicken Sie im Abschnitt Serverzertifikat für Objekt-Storage-API-Service-Endpunkte auf **Standardzertifikate verwenden**.
3. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

   Wenn Sie die Standard-Serverzertifikate für die Endpunkte der Objekt-Storage-API wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Die Standard-Serverzertifikate werden für alle nachfolgenden neuen API-Client-Verbindungen verwendet.

4. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

## Das CA-Zertifikat des StorageGRID-Systems wird kopiert

StorageGRID verwendet eine interne Zertifizierungsstelle (Certificate Authority, CA) zur Sicherung des internen Datenverkehrs. Dieses Zertifikat ändert sich nicht, wenn Sie Ihre eigenen Zertifikate hochladen.

**Was Sie benötigen**

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

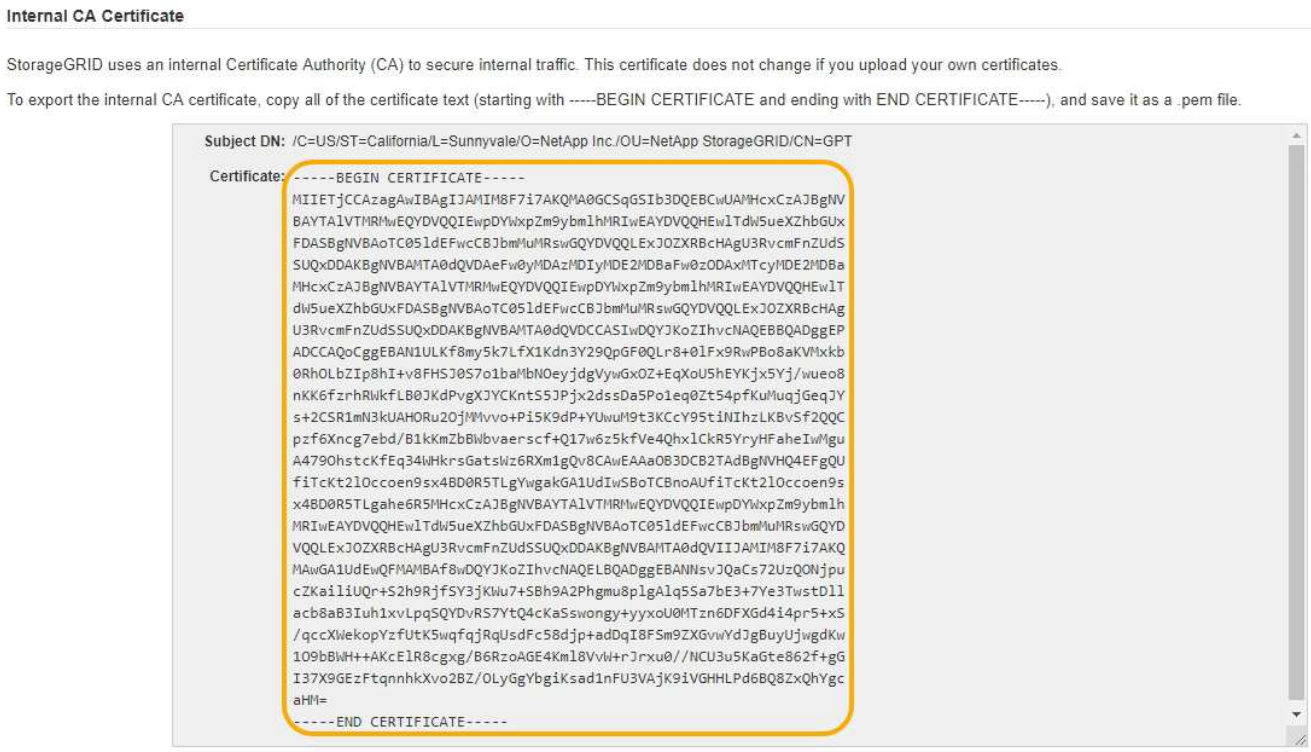
**Über diese Aufgabe**

Wenn ein benutzerdefiniertes Serverzertifikat konfiguriert wurde, sollten Client-Anwendungen den Server anhand des benutzerdefinierten Serverzertifikats überprüfen. Sie sollten das CA-Zertifikat nicht aus dem StorageGRID-System kopieren.

**Schritte**

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Wählen Sie im Abschnitt * Internes CA-Zertifikat* den gesamten Zertifikatstext aus.

   Sie müssen Folgendes einschließen `-----BEGIN CERTIFICATE-----` Und `-----END CERTIFICATE-----` Wählen Sie aus.




3. Klicken Sie mit der rechten Maustaste auf den ausgewählten Text, und wählen Sie **Kopieren**.
4. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.
5. Speichern Sie die Datei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

## Konfigurieren von StorageGRID-Zertifikaten für FabricPool

Bei S3-Clients, die eine strenge Hostname-Validierung durchführen und keine strenge Hostname-Validierung deaktivieren, z. B. ONTAP-Clients, die FabricPool verwenden, können Sie ein Serverzertifikat generieren oder hochladen, wenn Sie den Load Balancer-Endpunkt konfigurieren.

### Was Sie benötigen

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

### Über diese Aufgabe

Wenn Sie einen Load Balancer-Endpunkt erstellen, können Sie ein selbstsigniertes Serverzertifikat generieren oder ein Zertifikat hochladen, das von einer bekannten Zertifizierungsstelle (CA) signiert ist. In Produktionsumgebungen sollten Sie ein Zertifikat verwenden, das von einer bekannten Zertifizierungsstelle signiert ist. Von einer Zertifizierungsstelle signierte Zertifikate können unterbrechungsfrei gedreht werden. Sie sind außerdem sicherer, weil sie einen besseren Schutz vor man-in-the-Middle-Angriffen bieten.

In den folgenden Schritten finden Sie allgemeine Richtlinien für S3-Clients, die FabricPool verwenden. Weitere Informationen und Verfahren finden Sie in den Anweisungen zum Konfigurieren von StorageGRID für FabricPool.

Der separate Connection Load Balancer (CLB)-Service auf Gateway-Nodes ist veraltet und wird nicht mehr für die Verwendung mit FabricPool empfohlen.

**Schritte**

1. Konfigurieren Sie optional eine HA-Gruppe (High Availability, Hochverfügbarkeit) für die Verwendung von FabricPool.
2. Einen S3-Load-Balancer-Endpunkt für FabricPool erstellen.

   Wenn Sie einen HTTPS-Load-Balancer-Endpunkt erstellen, werden Sie aufgefordert, Ihr Serverzertifikat, den privaten Zertifikatschlüssel und das CA-Bundle hochzuladen.

3. Fügen Sie StorageGRID als Cloud-Tier in ONTAP bei.

   Geben Sie den Endpunkt-Port des Load Balancer und den vollständig qualifizierten Domänennamen an, der im hochgeladenen CA-Zertifikat verwendet wird. Geben Sie dann das CA-Zertifikat ein.

   Wenn eine Zwischenzertifizierungsstelle das StorageGRID-Zertifikat ausgestellt hat, müssen Sie das Zertifikat der Zwischenzertifizierungsstelle vorlegen. Wenn das StorageGRID-Zertifikat direkt von der Root-CA ausgestellt wurde, müssen Sie das Root-CA-Zertifikat bereitstellen.

**Verwandte Informationen**

"Konfigurieren Sie StorageGRID für FabricPool"

## Erstellen eines selbstsignierten Serverzertifikats für die Managementoberfläche

Sie können ein Skript verwenden, um ein selbstsigniertes Serverzertifikat für Management-API-Clients zu generieren, die eine strenge Hostnamen-Validierung erfordern.

**Was Sie benötigen**

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:

**Über diese Aufgabe**

In Produktionsumgebungen sollten Sie ein Zertifikat verwenden, das von einer bekannten Zertifizierungsstelle (CA) signiert ist. Von einer Zertifizierungsstelle signierte Zertifikate können unterbrechungsfrei gedreht werden. Sie sind außerdem sicherer, weil sie einen besseren Schutz vor man-in-the-Middle-Angriffen bieten.

**Schritte**

1. Ermitteln Sie den vollständig qualifizierten Domänennamen (FQDN) jedes Admin-Knotens.
2. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

3. Konfigurieren Sie StorageGRID mit einem neuen selbstsignierten Zertifikat.

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - Für `--domains`, Verwenden Sie Platzhalter, um die vollständig qualifizierten Domänennamen aller Admin-Knoten darzustellen. Beispiel: `*.ui.storagegrid.example.com` Verwendet den Platzhalter * für die Darstellung `admin1.ui.storagegrid.example.com` Und `admin2.ui.storagegrid.example.com`.
   - Einstellen `--type` Bis `management` Zum Konfigurieren des Zertifikats, das von Grid Manager und Tenant Manager verwendet wird.
   - Die erstellten Zertifikate sind standardmäßig für ein Jahr (365 Tage) gültig und müssen vor Ablauf neu erstellt werden. Sie können das verwenden `--days` Argument zum Überschreiben des standardmäßigen Gültigkeitszeitraums.

     > Die Gültigkeitsdauer eines Zertifikats beginnt, wenn `make-certificate` Wird ausgeführt. Sie müssen sicherstellen, dass der Management-API-Client mit der gleichen Datenquelle wie StorageGRID synchronisiert wird. Andernfalls kann der Client das Zertifikat ablehnen.

     ```
     $ sudo make-certificate --domains *.ui.storagegrid.example.com --type
     management --days 365
     ```

     Die resultierende Ausgabe enthält das öffentliche Zertifikat, das vom Management-API-Client benötigt wird.

4. Wählen Sie das Zertifikat aus, und kopieren Sie es.

   Geben Sie DIE START- und DAS ENDE-Tags in Ihre Auswahl ein.

5. Melden Sie sich von der Eingabeaufforderung-Shell ab. `$ exit`
6. Bestätigen Sie, dass das Zertifikat konfiguriert wurde:
   a. Greifen Sie auf den Grid Manager zu.
   b. Wählen Sie **Konfiguration** > **Server Certificates** > **Management Interface Server Certificate** Aus.
7. Konfigurieren Sie den Management-API-Client so, dass er das öffentliche Zertifikat verwendet, das Sie kopiert haben. Geben Sie DIE START- und END-Tags an.

# Konfigurieren von Speicher-Proxy-Einstellungen

Wenn Sie Plattform-Services oder Cloud Storage-Pools verwenden, können Sie einen nicht transparenten Proxy zwischen Storage Nodes und den externen S3-Endpunkten konfigurieren. Beispielsweise benötigen Sie einen nicht transparenten Proxy, um Meldungen von Plattformdiensten an externe Endpunkte, z. B. einen Endpunkt im Internet, zu senden.

**Was Sie benötigen**

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

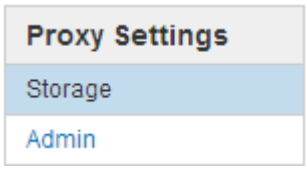
**Über diese Aufgabe**

Sie können die Einstellungen für einen einzelnen Speicherproxy konfigurieren.

**Schritte**

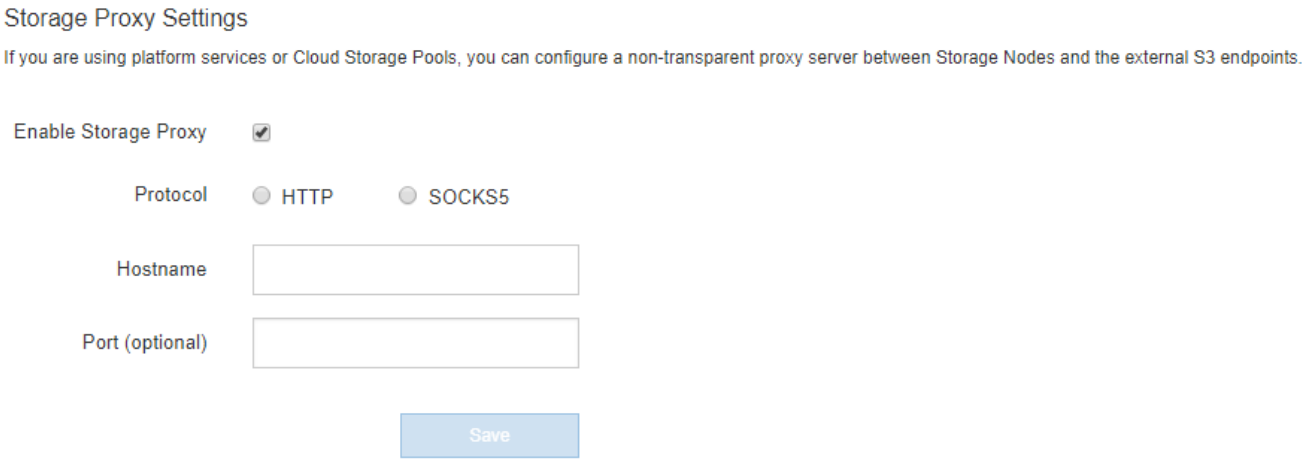
1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Proxy-Einstellungen**.

   Die Seite Speicher-Proxy-Einstellungen wird angezeigt. Standardmäßig ist **Storage** im Sidebar-Menü ausgewählt.




2. Aktivieren Sie das Kontrollkästchen * Storage Proxy aktivieren*.

   Die Felder zum Konfigurieren eines Speicher-Proxys werden angezeigt.




3. Wählen Sie das Protokoll für den nicht-transparenten Speicher-Proxy aus.
4. Geben Sie den Hostnamen oder die IP-Adresse des Proxy-Servers ein.
5. Geben Sie optional den Port ein, der für die Verbindung mit dem Proxyserver verwendet wird.

   Sie können dieses Feld leer lassen, wenn Sie den Standardport für das Protokoll verwenden: 80 für HTTP oder 1080 für SOCKS5.

6. Klicken Sie Auf **Speichern**.

   Nach dem Speichern des Storage-Proxy können neue Endpunkte für Plattformservices oder Cloud-Storage-Pools konfiguriert und getestet werden.

   Änderungen an Proxy können bis zu 10 Minuten in Anspruch nehmen.

7. Überprüfen Sie die Einstellungen Ihres Proxy-Servers, um sicherzustellen, dass für den Plattformdienst bezogene Nachrichten von StorageGRID nicht blockiert werden.

**Nachdem Sie fertig sind**

Wenn Sie einen Speicher-Proxy deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Storage Proxy aktivieren** und klicken Sie auf **Speichern**.

**Verwandte Informationen**

"Networking und Ports für Plattform-Services"

"Objektmanagement mit ILM"

# Konfigurieren von Administrator-Proxy-Einstellungen

Wenn Sie AutoSupport-Meldungen über HTTP oder HTTPS senden, können Sie einen nicht transparenten Proxy-Server zwischen Admin-Knoten und dem technischen Support (AutoSupport) konfigurieren.

**Was Sie benötigen**

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

**Über diese Aufgabe**

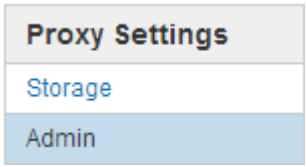
Sie können die Einstellungen für einen einzigen Admin-Proxy konfigurieren.

**Schritte**

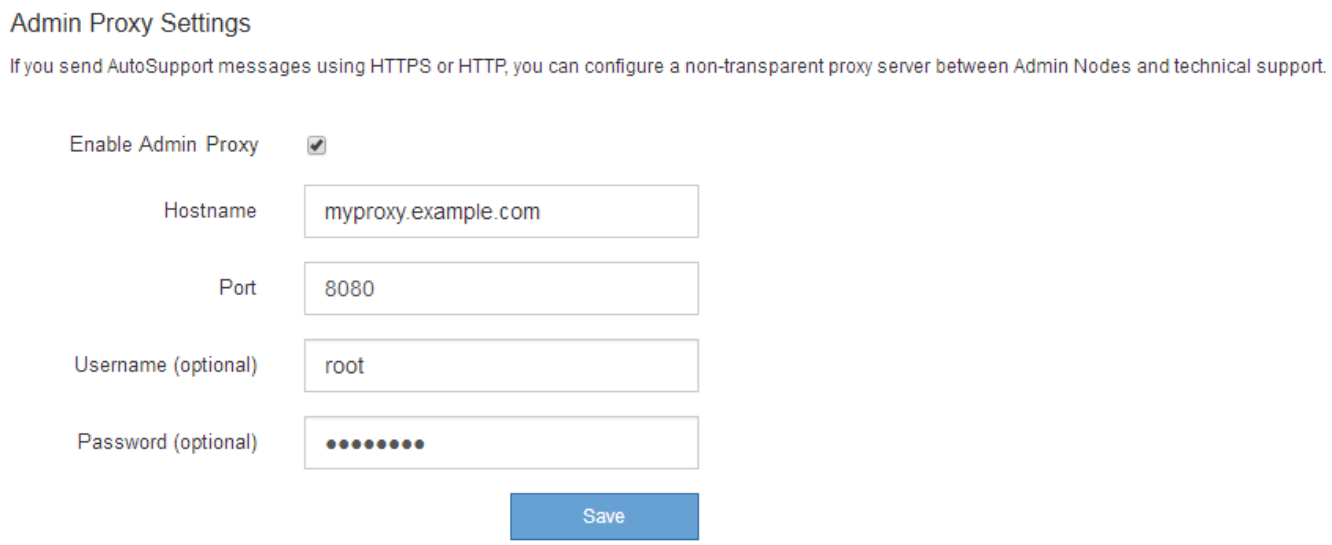
1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Proxy-Einstellungen**.

   Die Seite Admin Proxy Settings wird angezeigt. Standardmäßig ist **Storage** im Sidebar-Menü ausgewählt.

2. Wählen Sie im Sidebar-Menü die Option **Admin**.




3. Aktivieren Sie das Kontrollkästchen * Admin Proxy aktivieren*.




4. Geben Sie den Hostnamen oder die IP-Adresse des Proxy-Servers ein.
5. Geben Sie den Port ein, der für die Verbindung mit dem Proxy-Server verwendet wird.
6. Geben Sie optional den Proxy-Benutzernamen ein.

   Lassen Sie dieses Feld leer, wenn Ihr Proxy-Server keinen Benutzernamen benötigt.

7. Geben Sie optional das Proxy-Kennwort ein.

   Lassen Sie dieses Feld leer, wenn Ihr Proxy-Server kein Passwort benötigt.

8. Klicken Sie Auf **Speichern**.

   Nachdem der Admin-Proxy gespeichert wurde, wird der Proxy-Server zwischen Admin-Nodes und dem technischen Support konfiguriert.

   Änderungen an Proxy können bis zu 10 Minuten in Anspruch nehmen.

9. Wenn Sie den Proxy deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Admin Proxy aktivieren** und klicken Sie auf **Speichern**.

**Verwandte Informationen**

"Angeben des Protokolls für AutoSupport Meldungen"

# Verwalten von Richtlinien für die Verkehrsklassifizierung

Zur Verbesserung Ihrer QoS-Angebote (Quality of Service) können Sie Richtlinien zur Traffic-Klassifizierung erstellen, um verschiedene Arten von Netzwerkverkehr zu identifizieren und zu überwachen. Diese Richtlinien unterstützen die Begrenzung und das Monitoring des Datenverkehrs.

Richtlinien zur Traffic-Klassifizierung werden auf Endpunkte im StorageGRID Load Balancer Service für Gateway-Knoten und Admin-Nodes angewendet. Zum Erstellen von Richtlinien für die Verkehrsklassifizierung müssen Sie bereits Load Balancer Endpunkte erstellt haben.

## Passende Regeln und optionale Grenzen

Jede Traffic-Klassifizierungsrichtlinie enthält mindestens eine übereinstimmende Regel, um den Netzwerkverkehr zu identifizieren, der mit einer oder mehreren der folgenden Einheiten in Verbindung steht:

- Buckets
- Mandanten
- Subnetze (IPv4-Subnetze, in denen der Client enthalten ist)
- Endpunkte (Load Balancer Endpunkte)

StorageGRID überwacht den Datenverkehr, der mit allen Regeln innerhalb der Richtlinie im Einklang mit den Zielen der Regel steht. Jeder Traffic, der einer Richtlinie entspricht, wird von dieser Richtlinie übernommen. Umgekehrt können Sie Regeln festlegen, die mit dem gesamten Verkehr übereinstimmen, außer einer angegebenen Einheit.

Optional können Sie Obergrenzen für eine Richtlinie auf Basis der folgenden Parameter festlegen:

- Aggregat-Bandbreite In
- Horizontale Aggregatbandbreite
- Gleichzeitige Leseanforderungen
- Anforderungen Für Gleichzeitige Schreibvorgänge
- Bandbreite Pro Anfrage In
- Bandbreitenausforderung Pro Anfrage
- Leseanforderungsrate
- Schreibanforderungen-Rate

> Sie können Richtlinien erstellen, um die aggregierte Bandbreite zu begrenzen oder die Bandbreite nach Bedarf zu begrenzen. StorageGRID kann jedoch nicht beide Bandbreitenarten gleichzeitig einschränken. Eine Einschränkung der Bandbreite im Aggregat kann eine zusätzliche geringfügige Auswirkung auf die Performance des nicht begrenzten Datenverkehrs haben.

## Traffic-Beschränkung

Wenn Sie Traffic-Klassifizierungsrichtlinien erstellt haben, ist der Datenverkehr entsprechend der von Ihnen festgelegten Regeln und Grenzen begrenzt. Bei Bandbreitenbeschränkungen oder -Anforderungen werden die Anforderungen mit der von Ihnen festgelegten Rate in- oder Out-Streaming übertragen. StorageGRID kann nur eine Geschwindigkeit erzwingen. Daher ist die jeweils spezifischste Richtlinienabgleiche nach Matcher-Typ erzwungen. Bei allen anderen Grenzwerttypen werden Clientanforderungen um 250 Millisekunden verzögert und bei Anfragen, die die übereinstimmende Richtlinienbegrenzung überschreiten, eine langsame Antwort von 503 erhalten.

Im Grid Manager können Sie Traffic-Diagramme anzeigen und überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzen durchsetzen.

## Verwendung von Richtlinien für die Verkehrsklassifizierung mit SLAs

Sie können Richtlinien für die Traffic-Klassifizierung in Verbindung mit Kapazitätsgrenzen und Datensicherung verwenden, um Service Level Agreements (SLAs) durchzusetzen, die Besonderheiten bei Kapazität,

Datensicherung und Performance bieten.

Pro Load Balancer werden Einschränkungen für die Verkehrsklassifizierung implementiert. Wenn der Datenverkehr gleichzeitig auf mehrere Load Balancer verteilt wird, sind die maximalen Raten ein Vielfaches der von Ihnen angegebenen Ratenlimits.

Das folgende Beispiel zeigt drei SLA-Tiers. Sie können Traffic-Klassifizierungsrichtlinien erstellen, um die Performance-Ziele jeder SLA-Ebene zu erreichen.

| Service Level-Ebene | Kapazität | Datensicherung | Leistung | Kosten |
|---|---|---|---|---|
| Gold | 1 PB Speicherplatz zulässig | 3 ILM-Regel für Kopien | 25 K Anfragen/Sek.<br><br>5 GB/s (40 Gbit/s) Bandbreite | Kosten pro Monat |
| Silber | 250 TB Speicherplatz zulässig | ILM-Regel für 2 Kopien | 10 K Anfragen/Sek.<br><br>1.25 GB/s (10 Gbit/s) Bandbreite | Kosten pro Monat |
| Bronze | 100 TB Speicherplatz zulässig | ILM-Regel für 2 Kopien | 5 K Anfragen/Sek.<br><br>1 GB/s (8 Gbit/s) Bandbreite | Kosten pro Monat |

## Erstellen von Richtlinien zur Verkehrsklassifizierung

Sie erstellen Traffic-Klassifizierungsrichtlinien, wenn Sie den Netzwerkverkehr nach Bucket, Mandanten, IP-Subnetz oder Load Balancer-Endpunkt überwachen und optional begrenzen möchten. Optional können Sie Obergrenzen für eine Richtlinie basierend auf der Bandbreite, der Anzahl gleichzeitiger Anfragen oder der Anfragerate festlegen.

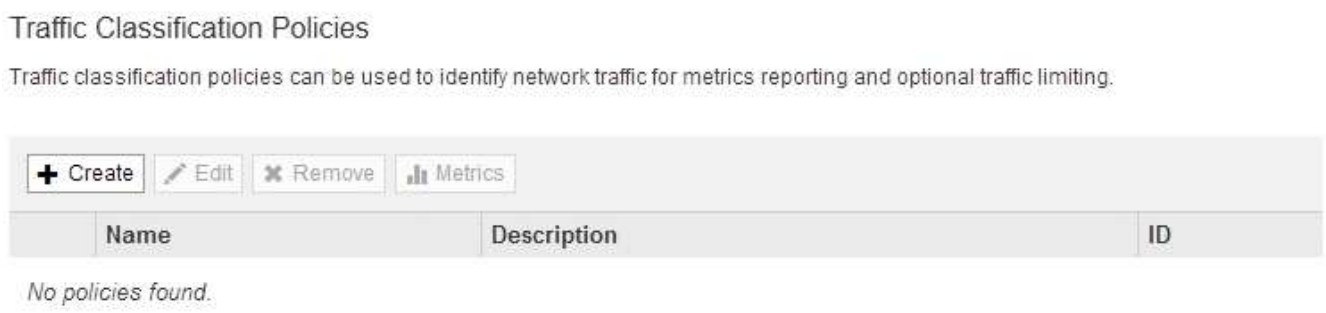
**Was Sie benötigen**

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen alle Load Balancer-Endpunkte erstellt haben, die übereinstimmen sollen.
- Sie müssen alle Mandanten erstellt haben, denen Sie entsprechen möchten.

**Schritte**

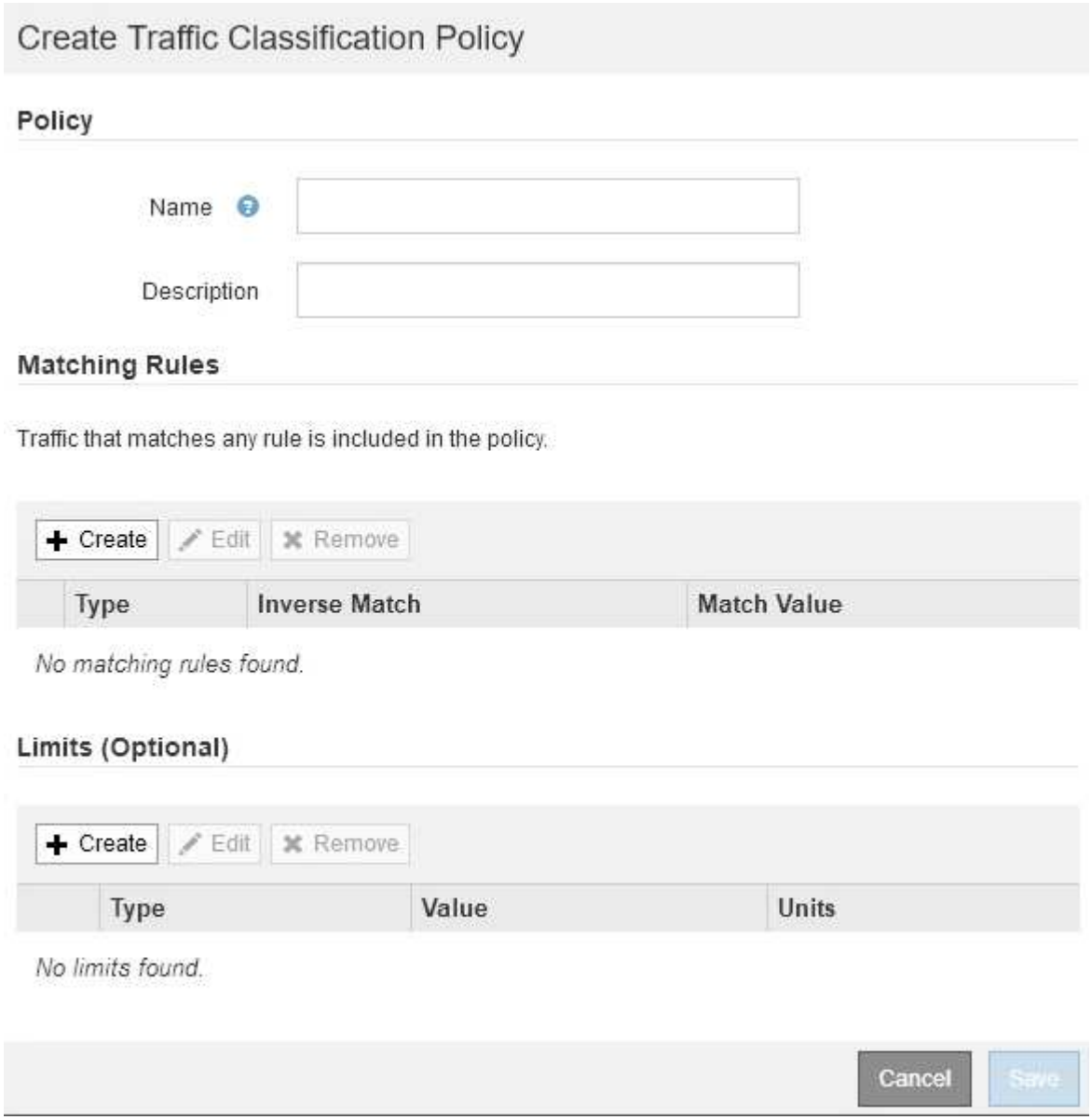
1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Verkehrsklassifizierung**.

   Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt.




2. Klicken Sie Auf **Erstellen**.

   Das Dialogfeld Richtlinie zur Verkehrsklassifizierung erstellen wird angezeigt.




3. Geben Sie im Feld **Name** einen Namen für die Richtlinie ein.

   Geben Sie einen beschreibenden Namen ein, damit Sie die Richtlinie erkennen können.

4. Fügen Sie optional eine Beschreibung für die Richtlinie im Feld **Beschreibung** hinzu.

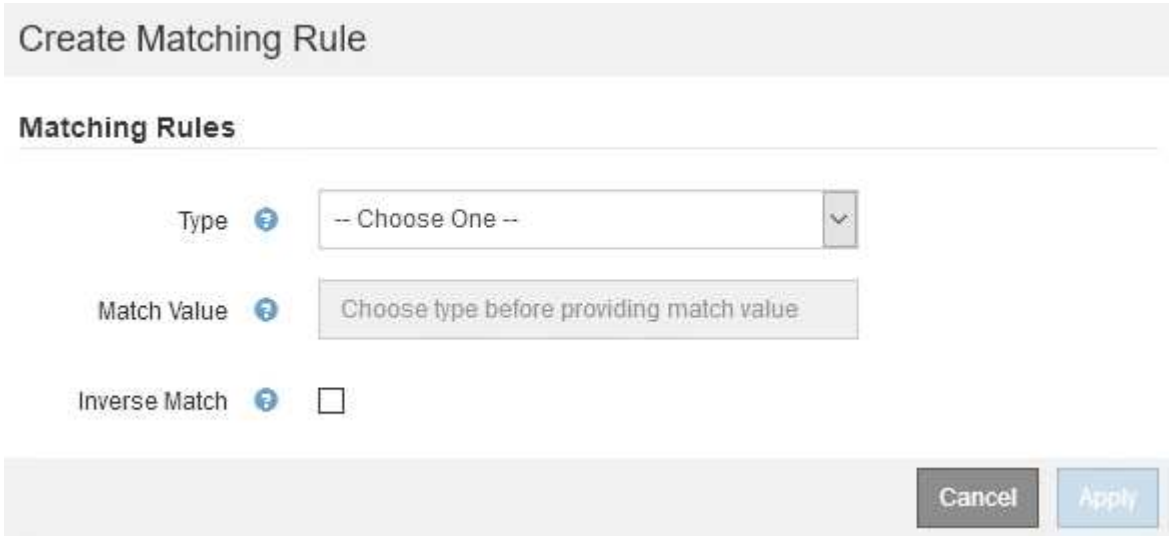
   Beschreiben Sie beispielsweise, auf welche Weise diese Richtlinie zur Klassifizierung von Verkehrsdaten zutrifft und welche Begrenzung sie hat.

5. Erstellen Sie eine oder mehrere passende Regeln für die Richtlinie.

   Die übereinstimmenden Regeln steuern, welche Einheiten von dieser Traffic-Klassifizierungsrichtlinie betroffen sein werden. Wählen Sie beispielsweise Tenant aus, wenn diese Richtlinie auf den Netzwerkverkehr für einen bestimmten Mandanten angewendet werden soll. Oder wählen Sie Endpunkt aus, wenn diese Richtlinie auf den Netzwerkverkehr auf einem bestimmten Load Balancer-Endpunkt angewendet werden soll.

   a. Klicken Sie im Abschnitt **passende Regeln** auf **Erstellen**.

      Das Dialogfeld „passende Regel erstellen“ wird angezeigt.

   b. Wählen Sie im Dropdown-Menü **Typ** den Typ der Entität aus, die in die übereinstimmende Regel aufgenommen werden soll.
   c. Geben Sie im Feld **Match-Wert** einen Match-Wert basierend auf dem gewählten Entitätstyp ein.
      - Bucket: Geben Sie einen Bucket-Namen ein.
      - Bucket-Regex: Geben Sie einen regulären Ausdruck ein, der für eine Reihe von Bucket-Namen verwendet wird.

        Der reguläre Ausdruck ist nicht verankert. Verwenden Sie den ^-Anker, um am Anfang des Bucket-Namens zu entsprechen, und verwenden Sie den €-Anker, um am Ende des Namens zu entsprechen.

      - CIDR: Geben Sie ein IPv4-Subnetz in CIDR-Notation ein, das dem gewünschten Subnetz entspricht.
      - Endpunkt: Wählen Sie einen Endpunkt aus der Liste der vorhandenen Endpunkte aus. Dies sind die Load Balancer Endpunkte, die Sie auf der Seite Load Balancer Endpoints definiert haben.
      - Mandant: Wählen Sie einen Mandanten aus der Liste der bestehenden Mandanten aus. Die Zuordnung von Mandanten basiert auf dem Besitz des Buckets, auf dem zugegriffen wird. Der anonyme Zugriff auf einen Bucket entspricht dem Mandanten, der den Bucket besitzt.

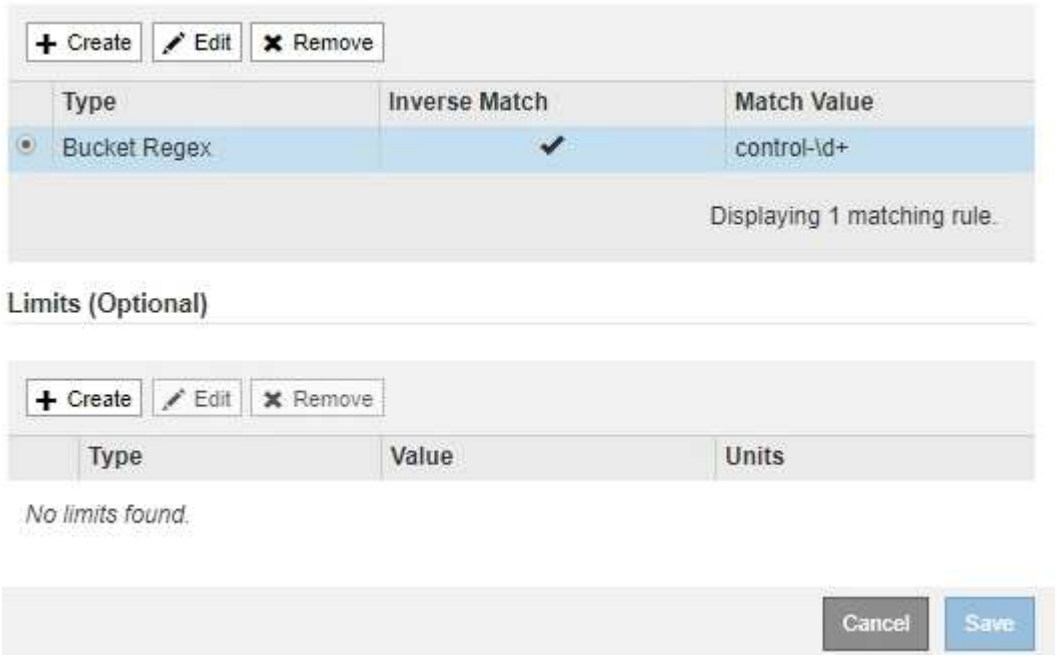
d. Wenn Sie dem gesamten Netzwerkverkehr *außer* Traffic entsprechen möchten, der mit dem gerade definierten Typ- und Vergleichswert übereinstimmt, aktivieren Sie das Kontrollkästchen **inverse**. Lassen Sie andernfalls das Kontrollkästchen nicht ausgewählt.

   Wenn diese Richtlinie beispielsweise auf alle Endpunkte des Load Balancer angewendet werden soll, geben Sie den zu ausgeschlossenen Endpunkt für den Load Balancer an und wählen Sie **Inverse** aus.

   Bei einer Richtlinie, die mehrere Matriken enthält, bei denen mindestens eine inverse Matrix ist, sollten Sie darauf achten, keine Richtlinie zu erstellen, die allen Anforderungen entspricht.

e. Klicken Sie Auf **Anwenden**.

   Die Regel wird erstellt und in der Tabelle Abpassende Regeln aufgeführt.




a. Wiederholen Sie diese Schritte für jede Regel, die Sie für die Richtlinie erstellen möchten.

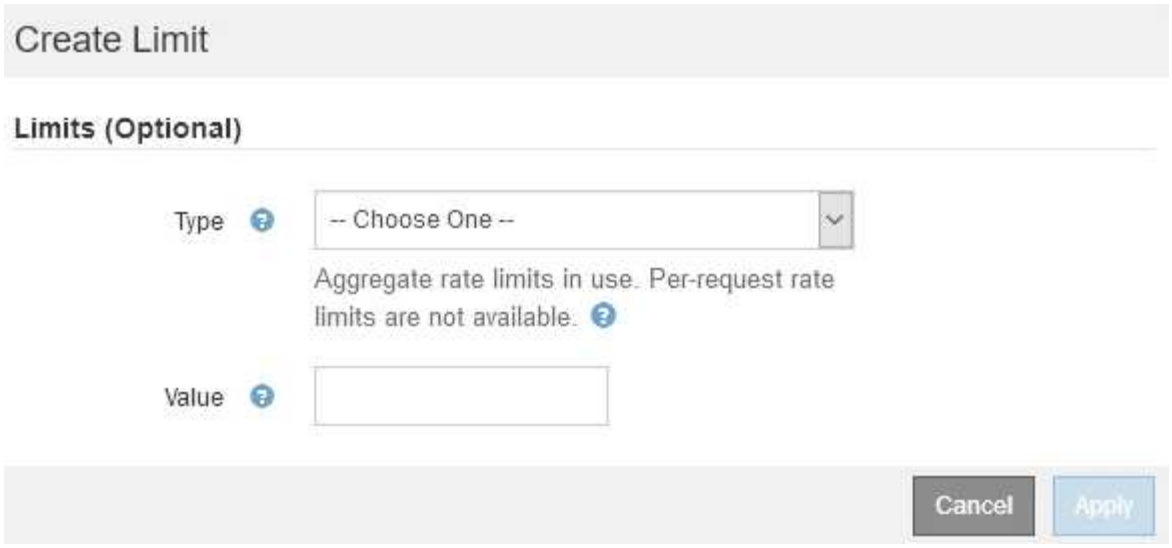
   Datenverkehr, der einer Regel entspricht, wird von der Richtlinie übernommen.

6. Optional können Grenzen für die Richtlinie erstellt werden.

   Selbst wenn Sie keine Grenzen erstellen, sammelt StorageGRID Metriken, sodass Sie den Netzwerk-Traffic, der der Richtlinie entspricht, überwachen können.

   a. Klicken Sie im Abschnitt **Limits** auf **Erstellen**.

      Das Dialogfeld Limit erstellen wird angezeigt.




b. Wählen Sie im Dropdown-Menü **Typ** den Grenzwert aus, den Sie auf die Richtlinie anwenden möchten.

   In der folgenden Liste bezieht sich **in** auf Datenverkehr von S3- oder Swift-Clients auf den StorageGRID-Load-Balancer, und **out** bezieht sich auf den Datenverkehr vom Load Balancer auf S3- oder Swift-Clients.

   - Aggregat-Bandbreite In
   - Horizontale Aggregatbandbreite
   - Gleichzeitige Leseanforderungen
   - Anforderungen Für Gleichzeitige Schreibvorgänge
   - Bandbreite Pro Anfrage In
   - Bandbreitenausforderung Pro Anfrage
   - Leseanforderungsrate
   - Schreibanforderungen-Rate

   > Sie können Richtlinien erstellen, um die aggregierte Bandbreite zu begrenzen oder die Bandbreite nach Bedarf zu begrenzen. StorageGRID kann jedoch nicht beide Bandbreitenarten gleichzeitig einschränken. Eine Einschränkung der Bandbreite im Aggregat kann eine zusätzliche geringfügige Auswirkung auf die Performance des nicht begrenzten Datenverkehrs haben.

   Bei Bandbreitenbeschränkungen wendet StorageGRID die Richtlinie an, die der jeweils festgelegten Grenzwertart am besten entspricht. Wenn Sie beispielsweise eine Richtlinie haben, die Datenverkehr in nur eine Richtung begrenzt, ist der Datenverkehr in die entgegengesetzte Richtung unbegrenzt, selbst wenn der Datenverkehr mit zusätzlichen Richtlinien mit Bandbreitenbeschränkungen übereinstimmt. StorageGRID implementiert „`Best`"-Übereinstimmungen für Bandbreiteneinschränkungen in der folgenden Reihenfolge:

   - Exakte IP-Adresse (/32-Maske)
   - Exakter Bucket-Name
   - Eimer-Regex
   - Mandant

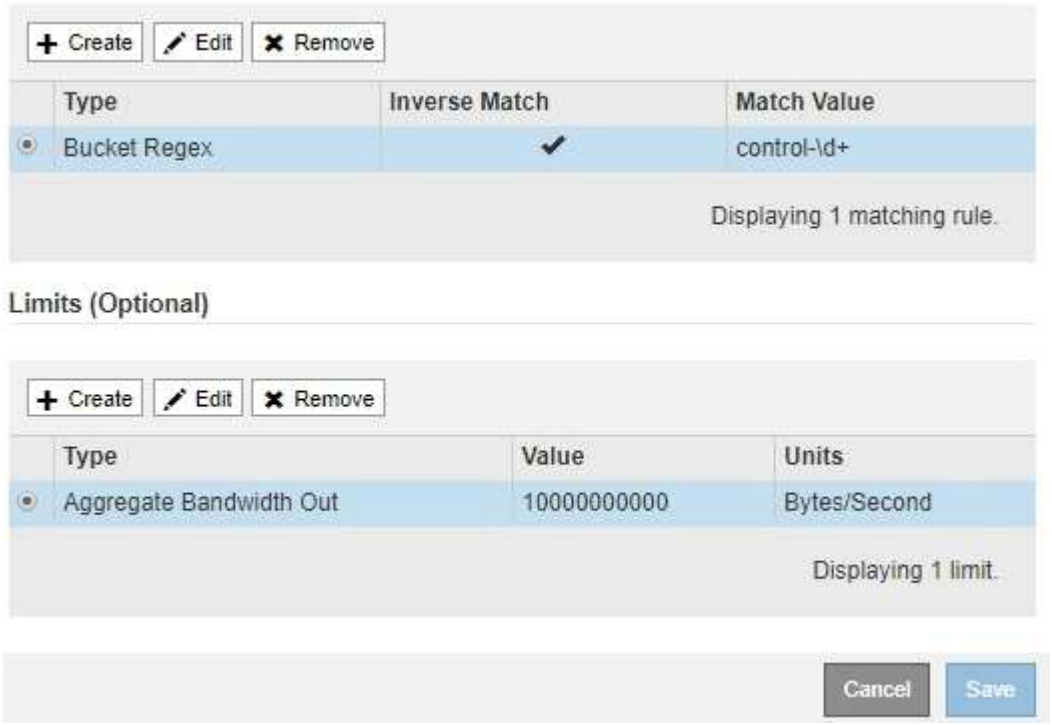
- Endpunkt
- Nicht exakte CIDR-Übereinstimmungen (nicht /32)
- Umgekehrte Übereinstimmungen

c. Geben Sie im Feld **Wert** einen numerischen Wert für den gewählten Grenzwert ein.

   Die erwarteten Einheiten werden angezeigt, wenn Sie ein Limit auswählen.

d. Klicken Sie Auf **Anwenden**.

   Die Begrenzung wird erstellt und in der Grenzwertetabelle aufgelistet.



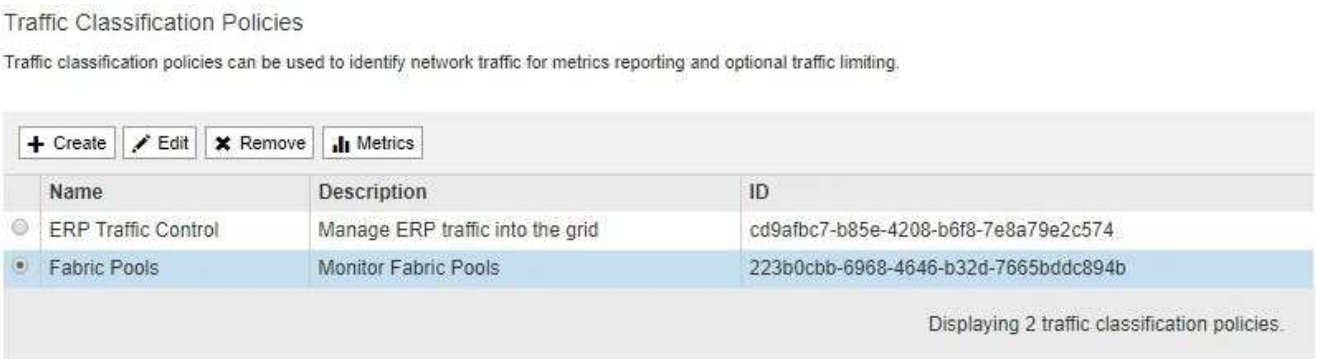

e. Wiederholen Sie diese Schritte für jedes Limit, das Sie der Richtlinie hinzufügen möchten.

   Wenn Sie beispielsweise ein Bandbreitenlimit von 40 Gbit/s für eine SLA-Ebene erstellen möchten, erstellen Sie eine aggregierte Bandbreitennutzung und ein Bandbreitenlimit und legen Sie jede auf 40 Gbit/s fest.

> Um Megabyte pro Sekunde in Gigabit pro Sekunde zu konvertieren, multiplizieren Sie mit acht. Beispielsweise entspricht 125 MB/s 1,000 Mbit/s oder 1 Gbit/s.

7. Wenn Sie mit dem Erstellen von Regeln und Grenzen fertig sind, klicken Sie auf **Speichern**.

   Die Richtlinie wird gespeichert und in der Tabelle „Richtlinien zur Klassifizierung von Verkehrsdaten“ aufgeführt.




Der S3- und Swift-Client-Traffic wird nun gemäß den Traffic-Klassifizierungsrichtlinien gehandhabt. Sie können Verkehrsdiagramme anzeigen und überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzwerte durchsetzen.

**Verwandte Informationen**

"Managen des Lastausgleichs"

"Anzeigen von Metriken zum Netzwerkverkehr"

## Bearbeiten einer Traffic-Klassifizierungsrichtlinie

Sie können eine Traffic-Klassifizierungsrichtlinie bearbeiten, um ihren Namen oder ihre Beschreibung zu ändern oder um Regeln oder Grenzen für die Richtlinie zu erstellen, zu bearbeiten oder zu löschen.

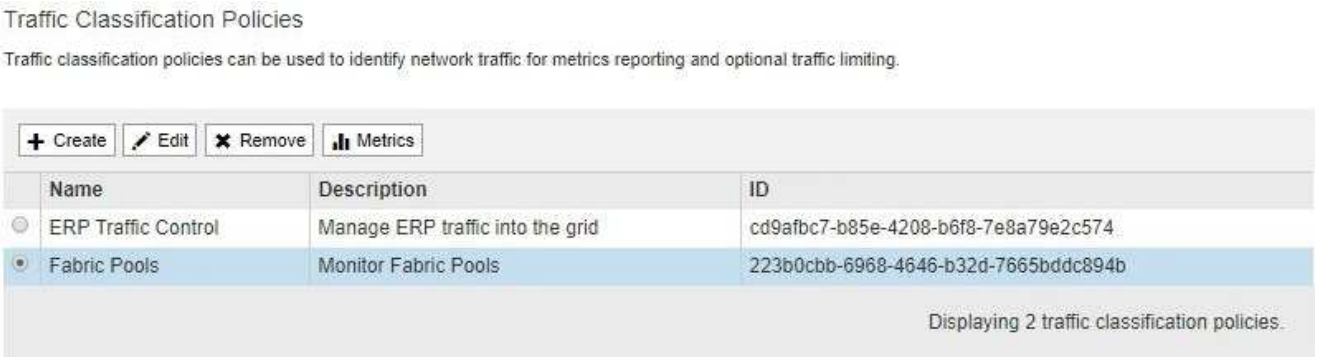
**Was Sie benötigen**

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

**Schritte**

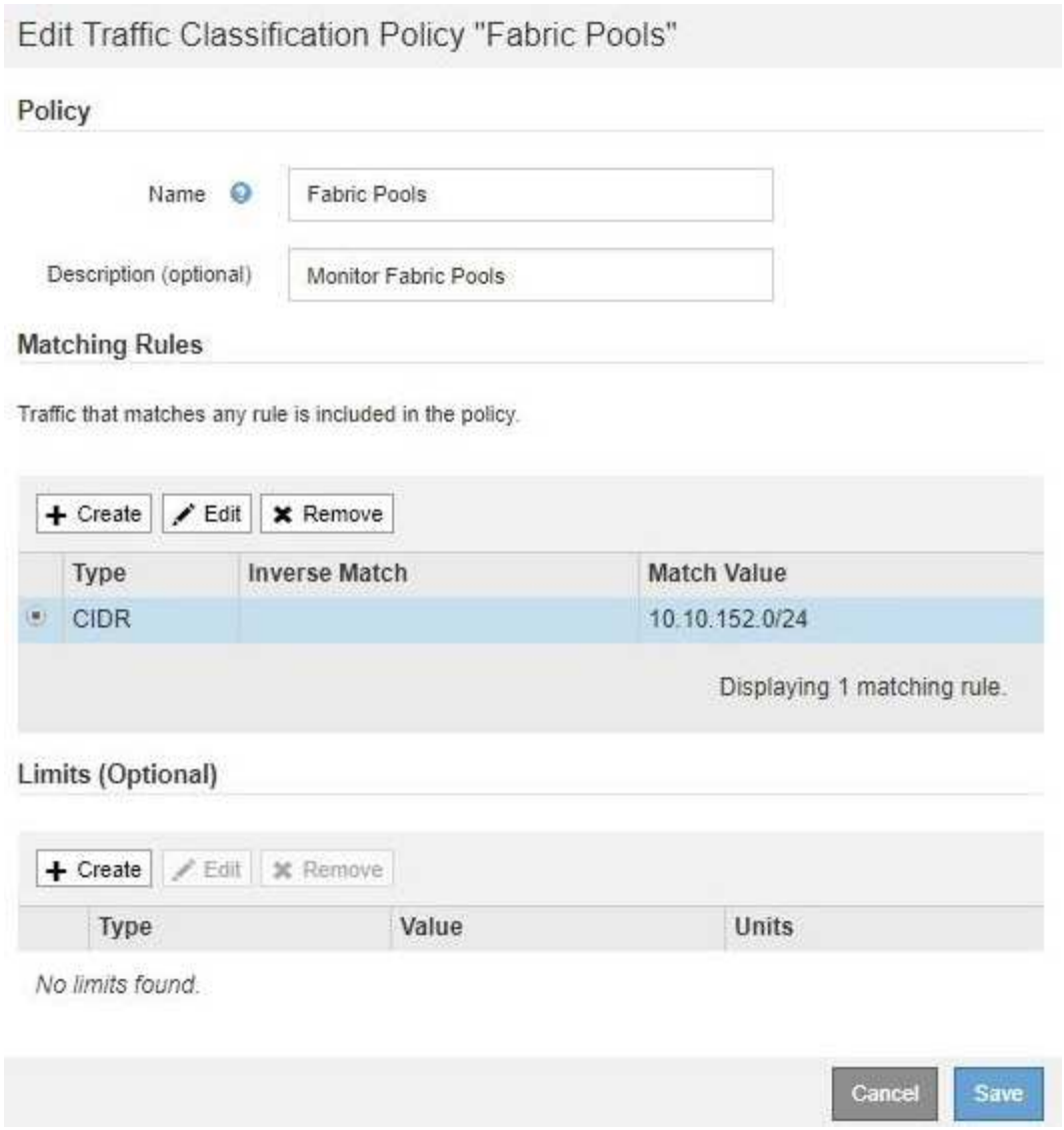
1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Verkehrsklassifizierung**.

   Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.




2. Wählen Sie das Optionsfeld links neben der Richtlinie, die Sie bearbeiten möchten.
3. Klicken Sie Auf **Bearbeiten**.

   Das Dialogfeld Richtlinie zur Klassifizierung von Datenverkehr bearbeiten wird angezeigt.




4. Erstellen, Bearbeiten oder Entfernen übereinstimmender Regeln und Grenzen nach Bedarf.
   a. Um eine übereinstimmende Regel oder ein entsprechendes Limit zu erstellen, klicken Sie auf **Erstellen** und befolgen Sie die Anweisungen zum Erstellen einer Regel oder zum Erstellen eines Limits.
   b. Um eine passende Regel oder Grenze zu bearbeiten, wählen Sie die Optionsschaltfläche für die Regel oder das Limit aus, klicken Sie im Abschnitt **passende Regeln** oder im Abschnitt **Grenzen** auf **Bearbeiten** und befolgen Sie die Anweisungen zum Erstellen einer Regel oder zum Erstellen eines Limits.
   c. Um eine passende Regel oder Begrenzung zu entfernen, wählen Sie die Optionsschaltfläche für die Regel oder die Begrenzung aus, und klicken Sie auf **Entfernen**. Klicken Sie dann auf **OK**, um zu bestätigen, dass Sie die Regel oder das Limit entfernen möchten.
5. Wenn Sie mit dem Erstellen oder Bearbeiten einer Regel oder eines Limits fertig sind, klicken Sie auf **Anwenden**.
6. Wenn Sie mit der Bearbeitung der Richtlinie fertig sind, klicken Sie auf **Speichern**.

   Die an der Richtlinie vorgenommenen Änderungen werden gespeichert, und der Netzwerkverkehr wird nun gemäß den Richtlinien zur Klassifizierung von Verkehrsmeldungen verarbeitet. Sie können Verkehrsdiagramme anzeigen und überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzwerte durchsetzen.

## Löschen einer Traffic-Klassifizierungsrichtlinie

Wenn Sie keine Traffic-Klassifizierungsrichtlinie mehr benötigen, können Sie sie löschen.

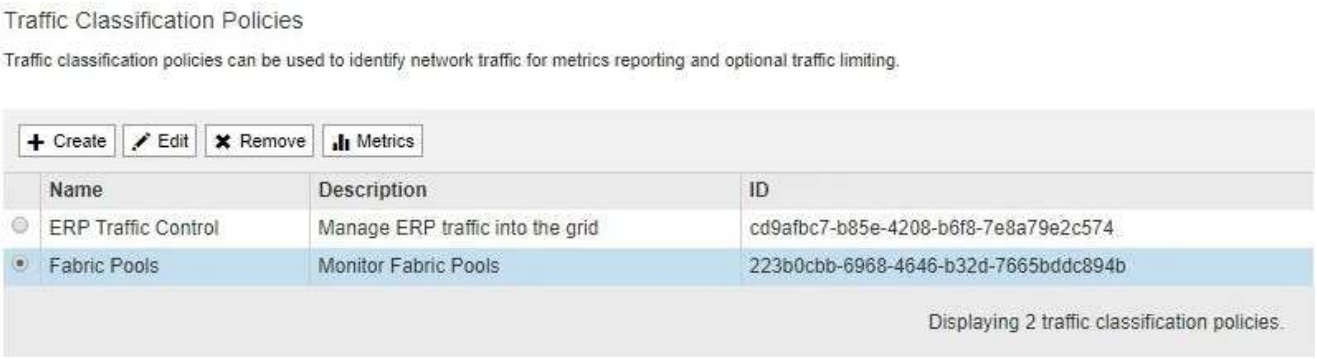
**Was Sie benötigen**

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

**Schritte**

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

   Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.




2. Wählen Sie das Optionsfeld links neben der Richtlinie, die Sie löschen möchten.
3. Klicken Sie Auf **Entfernen**.

   Ein Warndialogfeld wird angezeigt.


4. Klicken Sie auf **OK**, um zu bestätigen, dass Sie die Richtlinie löschen möchten.

   Die Richtlinie wird gelöscht.

## Anzeigen von Metriken zum Netzwerkverkehr

Sie können den Netzwerkverkehr überwachen, indem Sie die Diagramme aufrufen, die auf der Seite Richtlinien zur Klassifizierung von Verkehrsmeldungen verfügbar sind.

**Was Sie benötigen**

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

- Sie müssen über die Berechtigung Root Access verfügen.

**Über diese Aufgabe**

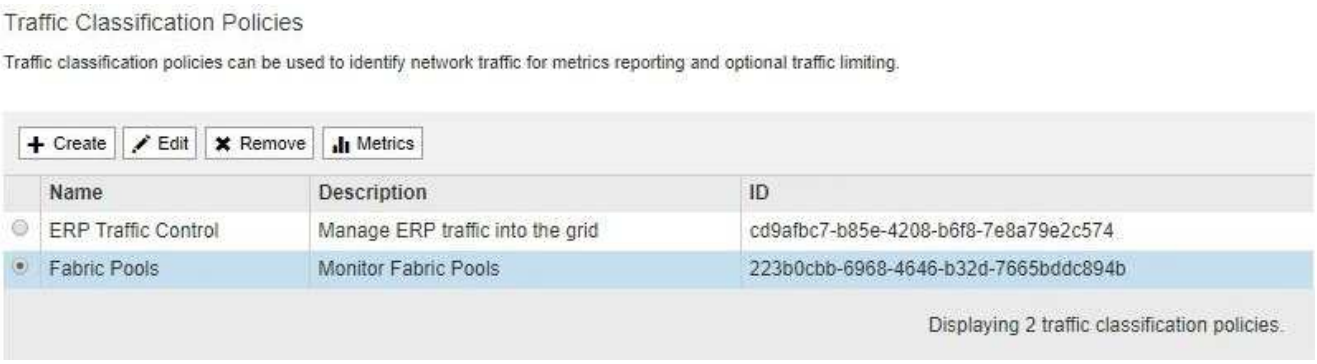
Für alle vorhandenen Traffic-Klassifizierungsrichtlinien können Sie Kennzahlen für den Load Balancer-Service anzeigen, um festzustellen, ob die Richtlinie den Datenverkehr im Netzwerk erfolgreich einschränkt. Anhand der Daten in den Diagrammen können Sie bestimmen, ob Sie die Richtlinie anpassen müssen.

Auch wenn für eine Richtlinie zur Klassifizierung von Datenverkehr keine Grenzen gesetzt wurden, werden Kennzahlen erfasst und die Diagramme bieten nützliche Informationen zum Verständnis von Verkehrstrends.

**Schritte**

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

   Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.




2. Wählen Sie das Optionsfeld links neben der Richtlinie, für die Sie Metriken anzeigen möchten.
3. Klicken Sie Auf **Metriken**.

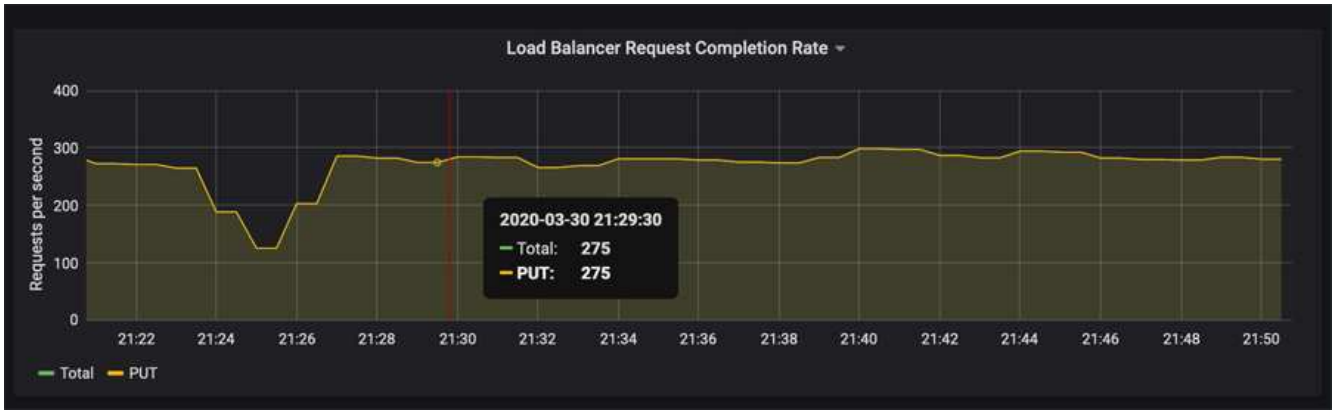
   Es wird ein neues Browserfenster geöffnet, und die Diagramme der Richtlinie zur Klassifizierung von Datenverkehr werden angezeigt. Die Diagramme zeigen Metriken nur für den Datenverkehr an, der mit der ausgewählten Richtlinie übereinstimmt.

   Sie können andere Richtlinien auswählen, die Sie anzeigen möchten, indem Sie das Pulldown-Menü **Policy** verwenden.

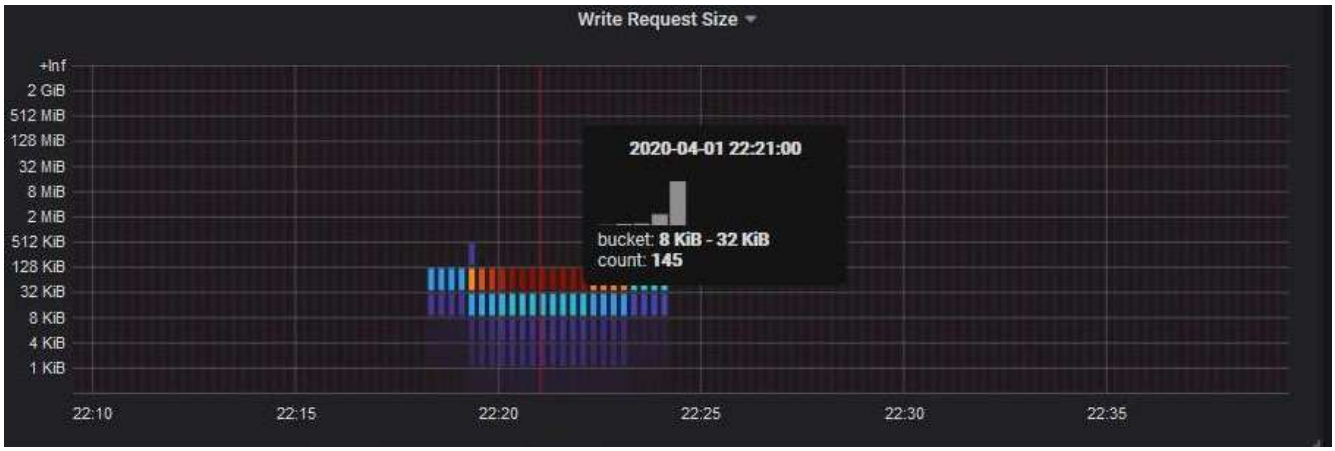

Die folgenden Diagramme sind auf der Webseite enthalten.

- Load Balancer Request Traffic: Dieses Diagramm liefert einen 3-minütigen Moving Average des Durchsatzes von Daten, die zwischen Load Balancer Endpunkten und den Clients, die die Anforderungen bearbeiten, in Bits pro Sekunde übertragen werden.
- Abschlusssatz für Lastbalancer-Anfragen: Dieses Diagramm bietet einen 3-minütigen Moving-Durchschnitt der Anzahl der abgeschlossenen Anfragen pro Sekunde, aufgeschlüsselt nach Anforderungstyp (GET, PUT, HEAD, DELETE). Dieser Wert wird aktualisiert, wenn die Kopfzeilen einer neuen Anfrage validiert wurden.
- Fehlerantwortzrate: Dieses Diagramm zeigt einen 3-minütigen Moving Average der Anzahl der an Kunden pro Sekunde zurückgegebenen Fehlerantworten, aufgeschlüsselt nach dem Fehlercode.
- Durchschnittliche Anfragedauer (nicht-Fehler): Dieses Diagramm bietet einen 3-minütigen Moving Average of Request durations, aufgeschlüsselt nach Anforderungstyp (GET, PUT, HEAD, DELETE). Jede Anforderungsdauer beginnt, wenn eine Anforderungs-Kopfzeile vom Lastbalancer-Dienst analysiert wird und endet, wenn der vollständige Antwortkörper an den Client zurückgesendet wird.
- Schreibanforderungsrate nach Objektgröße: Diese Heatmap bietet einen Moving Average von 3 Minuten für die Geschwindigkeit, mit der Schreibanforderungen basierend auf Objektgröße abgeschlossen werden. In diesem Zusammenhang beziehen sich Schreibanforderungen nur auf PUT-Anforderungen.
- Leseanforderungsrate nach Objektgröße: Dieser Heatmap bietet einen 3-minütigen Moving-Durchschnitt der Rate, mit der Leseanforderungen anhand der Objektgröße abgeschlossen werden. In diesem Zusammenhang beziehen sich Leseanforderungen nur auf ANFORDERUNGEN, DIE ABGERUFEN werden sollen. Die Farben in der Heatmap zeigen die relative Frequenz einer Objektgröße innerhalb eines einzelnen Diagramms an. Die kühleren Farben (z. B. violett und blau) zeigen niedrigere relative Raten an, und die wärmeren Farben (z. B. Orange und Rot) zeigen höhere relative Raten an.

4. Bewegen Sie den Cursor über ein Liniendiagramm, um ein Popup-Fenster mit Werten auf einem bestimmten Teil des Diagramms anzuzeigen.




5. Bewegen Sie den Mauszeiger über eine Heatmap, um ein Popup-Fenster mit Datum und Uhrzeit der Probe, Objektgrößen, die in die Anzahl aggregiert werden, und die Anzahl der Anfragen pro Sekunde in diesem Zeitraum anzuzeigen.




6. Verwenden Sie das Pull-down-Menü **Policy** oben links, um eine andere Richtlinie auszuwählen.

   Die Diagramme für die ausgewählte Richtlinie werden angezeigt.

7. Alternativ können Sie über das Menü * Support* auf die Diagramme zugreifen.
   a. Wählen Sie **Support** > **Tools** > **Metriken**.
   b. Wählen Sie im Abschnitt **Grafana** der Seite die Option **Traffic Classification Policy** aus.
   c. Wählen Sie die Richtlinie aus der Dropdown-Liste oben links auf der Seite aus.

      Richtlinien für die Verkehrsklassifizierung werden anhand ihrer ID identifiziert. Richtlinien-IDs sind auf der Seite Richtlinien zur Klassifizierung von Verkehrsdaten aufgeführt.

8. Analysieren Sie die Diagramme, um zu ermitteln, wie oft die Richtlinie den Datenverkehr einschränkt und ob Sie die Richtlinie anpassen müssen.

**Verwandte Informationen**

"Monitor Fehlerbehebung"

# Was sind Verbindungskosten

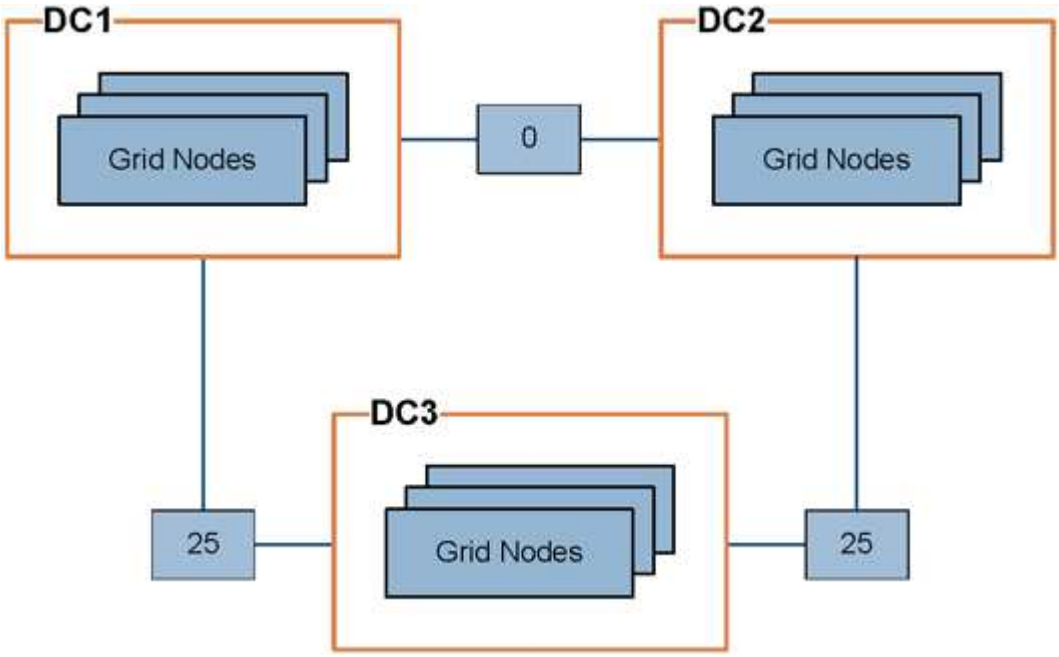
Durch die Verbindungskosten können Sie festlegen, welcher Datacenter-Standort einen angeforderten Service bereitstellt, wenn zwei oder mehr Datacenter-Standorte vorhanden

sind. Sie können die Verbindungskosten anpassen, um die Latenz zwischen Standorten reflektieren.

- Die Link-Kosten werden verwendet, um Prioritäten zu setzen, welche Objektkopie für die Bearbeitung von Objektabrufungen verwendet wird.
- Die Link-Kosten werden von der Grid-Management-API und der Mandanten-Management-API verwendet, um festzustellen, welche internen StorageGRID-Services verwendet werden sollen.
- Die Verbindungskosten werden vom CLB-Service auf Gateway-Knoten zur direkten Verbindung von Clients genutzt.

> Der CLB-Service ist veraltet.

Das Diagramm zeigt ein drei Standortraster mit Verbindungskosten, die zwischen Standorten konfiguriert sind:




- Der CLB-Service auf Gateway-Knoten verteilt Client-Verbindungen gleichermaßen auf alle Storage-Nodes am selben Datacenter-Standort und an beliebige Datacenter-Standorte mit einem Linkskosten von 0.

  Im Beispiel verteilt ein Gateway-Node am Datacenter-Standort 1 (DC1) Client-Verbindungen gleichmäßig auf Storage-Nodes an DC1 und Storage Nodes an DC2. Ein Gateway-Node bei DC3 sendet Client-Verbindungen nur zu Storage-Nodes an DC3.

- Beim Abrufen eines Objekts, das als mehrere replizierte Kopien vorhanden ist, ruft StorageGRID die Kopie im Datacenter ab, das die niedrigsten Verbindungskosten bietet.

  Wenn eine Client-Anwendung an DC2 ein Objekt abruft, das sowohl an DC1 als auch an DC3 gespeichert ist, wird das Objekt von DC1 abgerufen, da die Verbindungskosten von DC1 bis D2 0 sind, was niedriger ist als die Verbindungskosten von DC3 nach DC2 (25).

Verbindungskosten sind willkürliche relative Zahlen ohne spezifische Maßeinheit. So werden beispielsweise die Linkkosten von 50 weniger bevorzugt genutzt als eine Linkkosten von 25. In der Tabelle sind die häufig verwendeten Verbindungskosten aufgeführt.

| Verlinken | Verbindungskosten | Hinweise |
|---|---|---|
| Zwischen physischen Datacenter-Standorten zu wechseln | 25 (Standard) | Über WAN-Verbindung verbundene Datacenter. |
| Zwischen logischen Datacenter-Standorten am selben physischen Standort | 0 | Logische Rechenzentren befinden sich in demselben physischen Gebäude oder Campus, das über ein LAN verbunden ist. |

**Verwandte Informationen**

"Wie der Lastenausgleich funktioniert - CLB-Service"

## Verbindungskosten werden aktualisiert

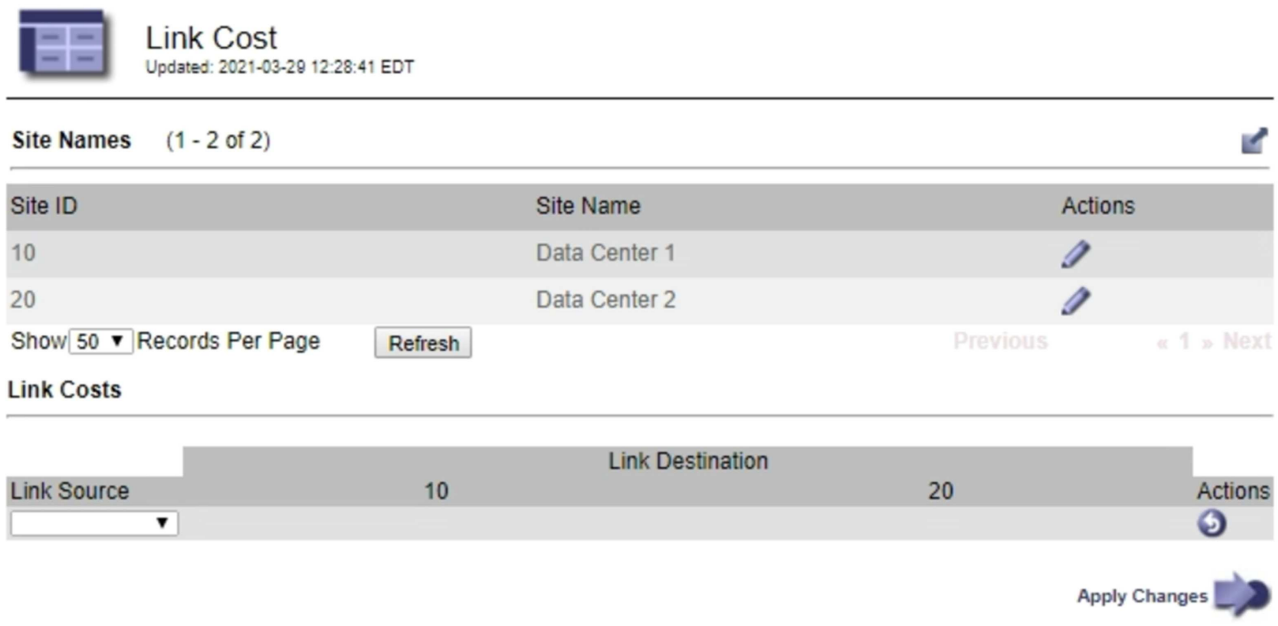
Sie können die Verbindungskosten zwischen Datacenter-Standorten aktualisieren, um die Latenz zwischen Standorten wiederzugeben.

**Was Sie benötigen**

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über die Berechtigung für die Konfiguration der Seite für die Grid-Topologie verfügen.

**Schritte**

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




2. Wählen Sie eine Website unter **Link Source** aus, und geben Sie unter **Link Destination** einen Kostenwert zwischen 0 und 100 ein.

   Sie können die Verbindungskosten nicht ändern, wenn die Quelle mit dem Ziel identisch ist.

Um Änderungen abzubrechen, klicken Sie auf **Zurücksetzen**.

3. Klicken Sie Auf **Änderungen Übernehmen**.

**Copyright-Informationen**

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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 IRGENDEINER 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.