



Netzwerke und Verbindungen verwalten

StorageGRID

NetApp
October 03, 2025

Inhalt

Netzwerke und Verbindungen verwalten	1
Richtlinien für StorageGRID-Netzwerke	1
Standard-StorageGRID-Netzwerke	1
Richtlinien	1
Optionale Schnittstellen	2
Zeigen Sie IP-Adressen an	2
Unterstützte Chiffren für ausgehende TLS-Verbindungen	3
Unterstützte Versionen von TLS	3
Unterstützte TLS 1.2-Cipher-Suiten	4
Unterstützte TLS 1.3-Cipher-Suiten	4
Netzwerkübertragungsverschlüsselung ändern	4
Verwalten von Richtlinien zur Verkehrsklassifizierung	5
Verwalten von Richtlinien zur Verkehrsklassifizierung	5
Richtlinien für die Verkehrsklassifizierung erstellen	7
Bearbeiten Sie eine Traffic-Klassifizierungsrichtlinie	13
Löschen einer Traffic-Klassifizierungsrichtlinie	15
Zeigen Sie Metriken zum Netzwerkverkehr an	15
Verwalten Sie Verbindungskosten	18
Was sind Verbindungskosten	19
Verbindungskosten aktualisieren	20

Netzwerke und Verbindungen verwalten

Richtlinien für StorageGRID-Netzwerke

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

Siehe [Konfiguration von S3- und Swift-Client-Verbindungen](#) Informationen zum Verbinden von S3 oder Swift Clients

Standard-StorageGRID-Netzwerke

Standardmäßig unterstützt StorageGRID drei Netzwerkschnittstellen pro Grid Node. So können Sie das Netzwerk für jeden einzelnen Grid Node so konfigurieren, dass er Ihren Sicherheits- und Zugriffsanforderungen entspricht.

Weitere Informationen zur Netzwerktopologie finden Sie unter [Netzwerkrichtlinien](#).

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	Schnittstellename
Raster	Eth0
Admin (optional)	Eth1

Netzwerk	Schnittstellename
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.

Optionale Schnittstellen

Optional können Sie einem Node zusätzliche Schnittstellen hinzufügen. Beispielsweise möchten Sie einem Admin- oder Gateway-Node eine Trunk-Schnittstelle hinzufügen, sodass Sie verwenden können [VLAN-Schnittstellen](#) Zur Trennung des Datenverkehrs von unterschiedlichen Applikationen oder Mandanten. Oder Sie möchten möglicherweise eine Zugriffsschnittstelle hinzufügen, die in A verwendet werden soll [Hochverfügbarkeitsgruppe \(High Availability Group, HA-Gruppe\)](#).

Informationen zum Hinzufügen von Trunk- oder Access-Schnittstellen finden Sie unter:

- **VMware (nach der Installation des Knotens):** [VMware: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node](#)
- **RHEL oder CentOS (vor dem Installieren des Knotens):** [Erstellen von Node-Konfigurationsdateien](#)
- **Ubuntu oder Debian (vor der Installation des Knotens):** [Erstellen von Node-Konfigurationsdateien](#)
- **RHEL, CentOS, Ubuntu oder Debian (nach der Installation des Knotens):** [Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node](#)

Zeigen Sie IP-Adressen an

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 sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).

Über diese Aufgabe

Informationen zum Ändern von IP-Adressen finden Sie unter [Recovery und Wartung](#).

Schritte

1. Wählen Sie **NODES Grid Node Übersicht** aus.
2. Wählen Sie **Mehr anzeigen** rechts neben dem Titel der IP-Adressen.

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

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state:  Connected

Storage used:

Object data		7%	?
Object metadata		5%	?

Software version: 11.6.0 (build 20210915.1941.afce2d9)

IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

Interface ^	IP address ^
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

Alerts

Alert name ^	Severity ? ^	Time triggered ^	Current values
ILM placement unachievable 🔗	 Major	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

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

Netzwerkübertragungsverschlüsselung ändern

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 sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben spezifische Zugriffsberechtigungen.

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 System Gitteroptionen**.
2. Ändern Sie im Abschnitt Netzwerkoptionen die Netzwerkübertragungsverschlüsselung in **AES128-SHA** oder **AES256-SHA** (Standardeinstellung).

Network Options

Prevent Client Modification  

Enable HTTP Connection  

Network Transfer Encryption  ☐ AES128-SHA ☒ AES256-SHA

3. Wählen Sie **Speichern**.

Verwalten von Richtlinien zur Verkehrsklassifizierung

Verwalten von Richtlinien zur 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.

Übereinstimmungsregeln

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.

Traffic-Beschränkung

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
- Schreibenanforderungen-Rate

Grenzwerte werden pro Load Balancer erzwungen. Wenn der Datenverkehr gleichzeitig auf mehrere Load Balancer verteilt wird, sind die maximalen Raten ein Vielfaches der von Ihnen angegebenen Ratenlimits.



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 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.

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. 5 GB/s (40 Gbit/s) Bandbreite	Kosten pro Monat
Silber	250 TB Speicherplatz zulässig	ILM-Regel für 2 Kopien	10 K Anfragen/Sek. 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. 1 GB/s (8 Gbit/s) Bandbreite	Kosten pro Monat

Richtlinien für die Verkehrsklassifizierung erstellen

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 sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben die Root-Zugriffsberechtigung.
- Sie haben alle Load Balancer-Endpunkte erstellt, die übereinstimmen sollen.
- Sie haben alle Mandanten erstellt, denen Sie entsprechen möchten.

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk Verkehrsklassifizierung**.

Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

Create

Edit

Remove

Metrics

Name	Description	ID
No policies found.		

2. Wählen Sie **Erstellen**.

Das Dialogfeld Richtlinie zur Verkehrsklassifizierung erstellen wird angezeigt.

Create Traffic Classification Policy

Policy

Name ⓘ

Description

Matching Rules

Traffic that matches any rule is included in the policy.

+ Create

✎ Edit

✕ Remove

Type	Inverse Match	Match Value
------	---------------	-------------

No matching rules found.

Limits (Optional)

+ Create

✎ Edit

✕ Remove

Type	Value	Units
------	-------	-------

No limits found.

Cancel

Save

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. Wählen Sie im Abschnitt **passende Regeln** die Option **Erstellen** aus.

Das Dialogfeld „passende Regel erstellen“ wird angezeigt.

Create Matching Rule

Matching Rules

Type ⓘ

-- Choose One --

Match Value ⓘ

Choose type before providing match value

Inverse Match ⓘ

☐

Cancel

Apply

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. Siehe [Konfigurieren von Load Balancer-Endpunkten](#).
 - 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. Wählen Sie **Anwenden**.

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

+ Create
Edit
Remove

Type	Inverse Match	Match Value
Bucket Regex	✓	control-ld+

Displaying 1 matching rule.

Limits (Optional)

+ Create
Edit
Remove

Type	Value	Type	Units
------	-------	------	-------

No limits found.

Cancel

Save

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. Wählen Sie im Abschnitt **Grenzwerte** die Option * Erstellen*.

Das Dialogfeld Limit erstellen wird angezeigt.

Create Limit

Limits (Optional)

Type
?
-- Choose One --

Aggregate rate limits in use. Per-request rate limits are not available. ?

Value
?

Cancel

Apply

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. Wählen Sie **Anwenden**.

Die Begrenzung wird erstellt und in der Grenzwertetabelle aufgelistet.

+ Create
✎ Edit
✕ Remove

Type	Inverse Match	Match Value
Bucket Regex	✓	control-ld+

Displaying 1 matching rule.

Limits (Optional)

+ Create
✎ Edit
✕ Remove

Type	Value	Units
Aggregate Bandwidth Out	10000000000	Bytes/Second

Displaying 1 limit.

Cancel
Save

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 Limits fertig sind, wählen Sie **Speichern**.

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

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create ✎ Edit ✕ Remove 📊 Metrics		
Name	Description	ID
ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

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. Siehe [Zeigen Sie Metriken zum Netzwerkverkehr an](#).

Bearbeiten Sie eine 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 sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben die Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk Verkehrsklassifizierung**.

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

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create Edit Remove Metrics			
	Name	Description	ID
☐	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
☒	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b
Displaying 2 traffic classification policies.			

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

Das Dialogfeld Richtlinie zur Klassifizierung von Datenverkehr bearbeiten wird angezeigt.

Edit Traffic Classification Policy "Fabric Pools"

Policy

Name

Fabric Pools

Description (optional)

Monitor Fabric Pools

Matching Rules

Traffic that matches any rule is included in the policy.

[+ Create](#) [Edit](#) [Remove](#)

Type	Inverse Match	Match Value
☒ CIDR		10.10.152.0/24

Displaying 1 matching rule.

Limits (Optional)

[+ Create](#) [Edit](#) [Remove](#)

Type	Value	Units
------	-------	-------

No limits found.

Cancel

Save

- Erstellen, Bearbeiten oder Entfernen übereinstimmender Regeln und Grenzen nach Bedarf.
 - Um eine übereinstimmende Regel oder ein entsprechendes Limit zu erstellen, wählen Sie **Erstellen** aus, und befolgen Sie die Anweisungen zum Erstellen einer Regel oder zum Erstellen eines Limits.
 - Um eine passende Regel oder Grenze zu bearbeiten, wählen Sie die Optionsschaltfläche für die Regel oder die Begrenzung aus, wählen Sie im Abschnitt **passende Regeln** oder im Abschnitt **Grenzen** die Option **Bearbeiten** und befolgen Sie die Anweisungen zum Erstellen einer Regel oder zum Erstellen eines Limits.
 - Um eine passende Regel oder Begrenzung zu entfernen, wählen Sie die Optionsschaltfläche für die Regel oder die Begrenzung aus, und wählen Sie **Entfernen**. Wählen Sie dann **OK** aus, um zu bestätigen, dass Sie die Regel oder das Limit entfernen möchten.
- Wenn Sie mit dem Erstellen oder Bearbeiten einer Regel oder eines Limits fertig sind, wählen Sie **Anwenden**.
- Wenn Sie mit der Bearbeitung der Richtlinie fertig sind, wählen Sie **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 sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben die Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk Verkehrsklassifizierung**.

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

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create Edit Remove Metrics

	Name	Description	ID
☐	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
☒	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bdc894b

Displaying 2 traffic classification policies.

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

Ein Warndialogfeld wird angezeigt.

 **Warning**

Delete Policy

Are you sure you want to delete the policy "Fabric Pools"?

Cancel OK

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

Die Richtlinie wird gelöscht.

Zeigen Sie Metriken zum Netzwerkverkehr an

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 sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).

- Sie verfügen über die Berechtigung Root Access oder die Berechtigungen für Mandantenkonten.

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 Netzwerk Verkehrsklassifizierung**.

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

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create Edit ✕ Remove Metrics			
	Name	Description	ID
☐	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
☒	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bdc894b
Displaying 2 traffic classification policies.			



Die Schaltflächen **Erstellen**, **Bearbeiten** und **Entfernen** sind deaktiviert, wenn Sie über die Berechtigung für Mandantenkonten verfügen, aber nicht über die Berechtigung Root-Zugriff verfügen.

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

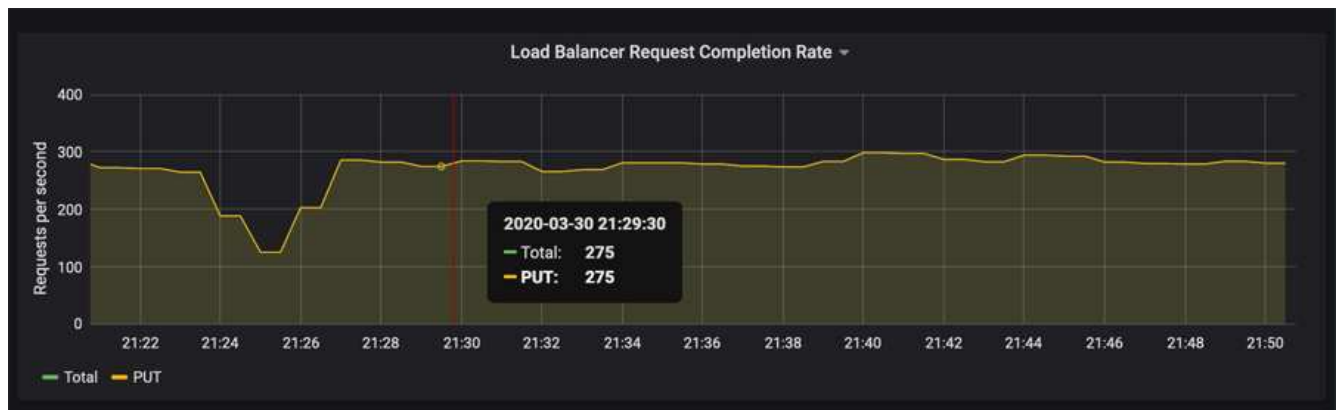
Sie können andere Richtlinien auswählen, die Sie anzeigen möchten, indem Sie das Pulldown-Menü **Policy** verwenden.



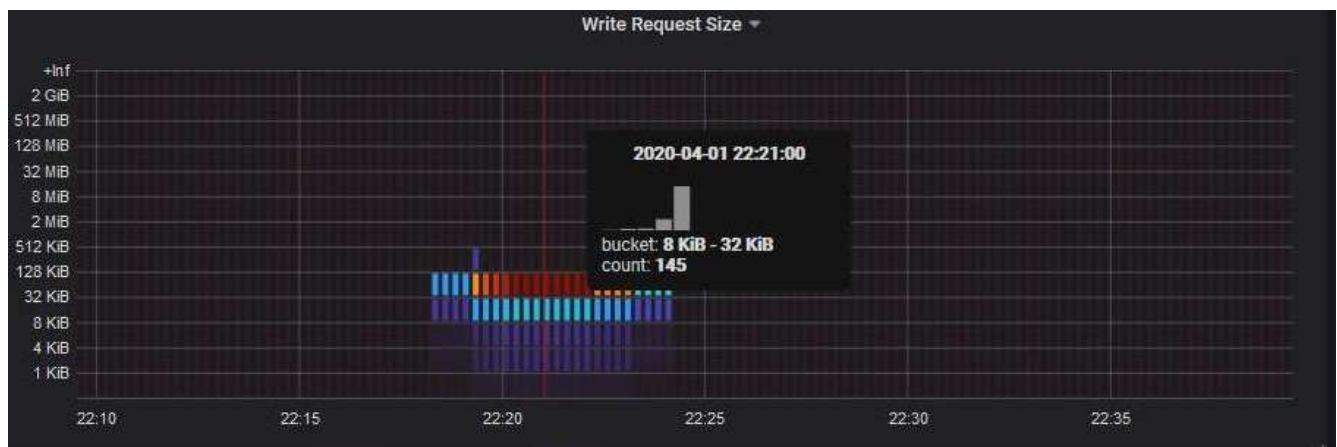
Die folgenden Diagramme sind auf der Webseite enthalten.

- **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.
- **Fehlerantwortrate:** 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 Kennzahlen** aus.
 - 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

[Monitoring und Fehlerbehebung](#)

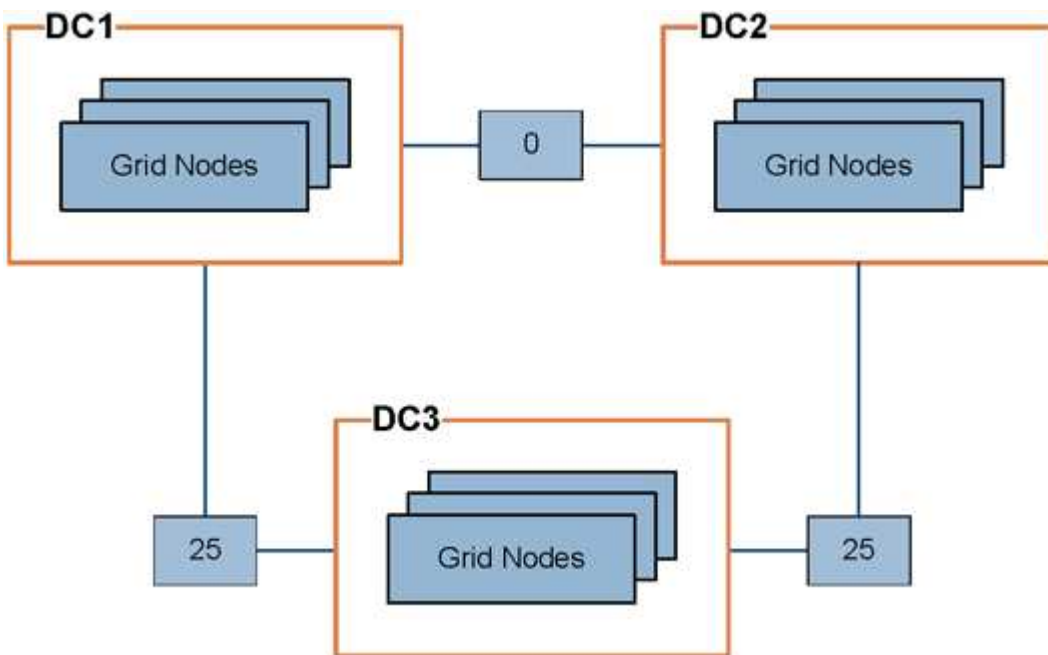
Verwalten Sie Verbindungskosten

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 veralteten Connection Load Balancer (CLB)-Dienst auf Gateway-Knoten zur direkten Weiterleitung von Client-Verbindungen verwendet. Siehe [Wie der Lastenausgleich funktioniert - CLB-Service](#).

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 abrufen, 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.

Verbindungskosten aktualisieren

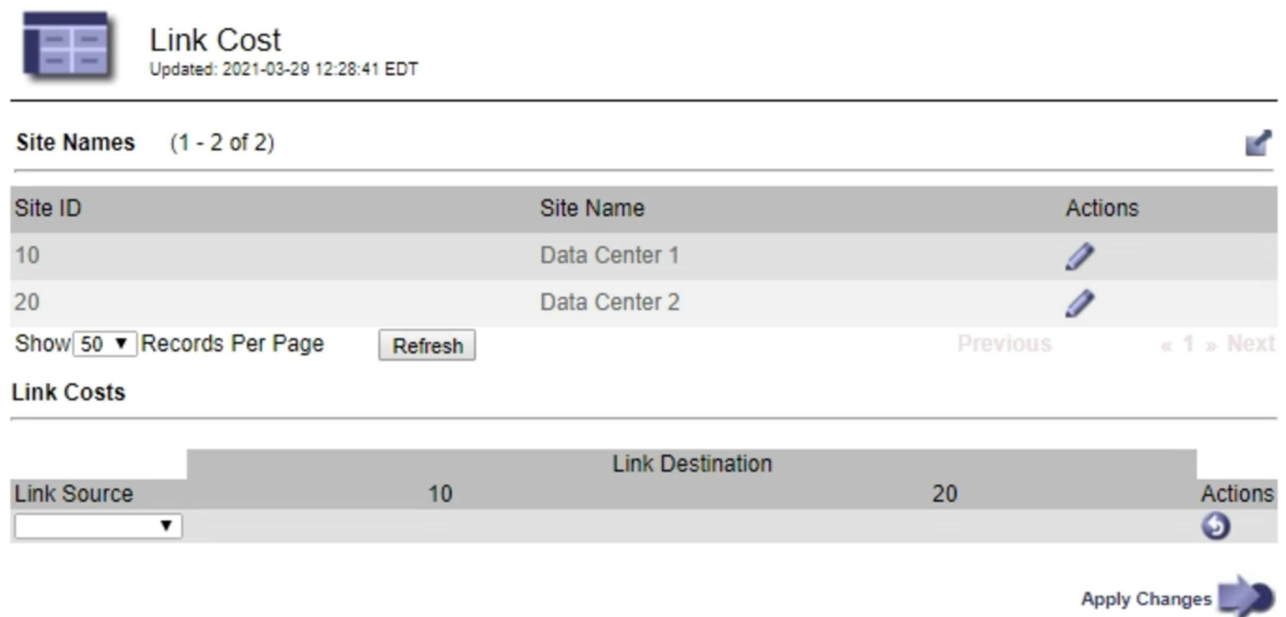
Sie können die Verbindungskosten zwischen Datacenter-Standorten aktualisieren, um die Latenz zwischen Standorten wiederzugeben.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben die Berechtigung für die Konfiguration der Seite Grid Topology.

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk Link Cost**.



Link Cost
Updated: 2021-03-29 12:28:41 EDT

Site Names (1 - 2 of 2)

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	

Show Records Per Page Previous « 1 » Next

Link Costs

Link Source	Link Destination	Actions
	10	20 



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 abubrechen, wählen Sie „  **Zurücksetzen**.

3. Wählen Sie **Änderungen Anwenden**.

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 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.