



Managen des Lastausgleichs

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

- Managen des Lastausgleichs 1
 - Wie funktioniert der Lastausgleich? Load Balancer Service 1
 - Konfigurieren von Load Balancer-Endpunkten 2
 - Wie der Lastenausgleich funktioniert - CLB-Service 10

Managen des Lastausgleichs

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

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

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



Der CLB-Service ist veraltet.

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

Wie funktioniert der Lastausgleich? Load Balancer Service

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

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

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

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

Überlegungen zu Ports

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

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



Der CLB-Service ist veraltet.

CPU-Verfügbarkeit

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

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

Verwandte Informationen

["Verwalten Sie erholen"](#)

Konfigurieren von Load Balancer-Endpunkten

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

Erstellen von Load Balancer-Endpunkten

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

Was Sie benötigen

- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Wenn Sie zuvor Ports neu zugeordnet haben, die Sie für den Load Balancer-Dienst verwenden möchten, müssen Sie die Neuzuordnungen entfernt haben.



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



Der CLB-Service ist veraltet.


Schritte

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

Die Seite Load Balancer Endpoints wird angezeigt.

Load Balancer Endpoints

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

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

 Add endpoint port  Edit endpoint  Remove endpoint port

Display name	Port	Using HTTPS
--------------	------	-------------

No endpoints configured.

2. Wählen Sie **Endpunkt hinzufügen**.

Das Dialogfeld Endpunkt erstellen wird angezeigt.

Create Endpoint

Display Name

Port

10443

Protocol

 HTTP HTTPS

Endpoint Binding Mode

 Global HA Group VIPs Node Interfaces

Cancel

Save

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

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



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

5. Wählen Sie **HTTP** oder **HTTPS** aus, um das Netzwerkprotokoll für diesen Endpunkt festzulegen.
6. Wählen Sie einen Endpunktbindungsmodus aus.
 - **Global** (Standard): Der Endpunkt ist auf allen Gateway Nodes und Admin Nodes auf der angegebenen Portnummer zugänglich.


Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

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

Cancel

Save

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

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

Create Endpoint

Display Name


Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

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

Displaying 2 HA groups.

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

Cancel

Save

- **Node-Schnittstellen:** Der Endpunkt ist nur auf den angegebenen Knoten und den Netzwerkschnittstellen zugänglich. In diesem Modus definierte Endpunkte können dieselbe Portnummer wiederverwenden, solange sich diese Schnittstellen nicht gegenseitig überschneiden.

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

Create Endpoint


Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

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

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

7. Wählen Sie **Speichern**.

Das Dialogfeld Endpunkt bearbeiten wird angezeigt.

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

Edit Endpoint Unsecured Port A (port 10449)

Endpoint Service Configuration

Endpoint service type S3 Swift

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

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

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

Load Certificate

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

Server Certificate

Certificate Private Key

CA Bundle

Cancel

Save

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

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

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

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

Die PEM-kodierten Zertifikatdaten für den Endpoint werden angezeigt.

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

Generate Certificate

Domain 1

IP 1

Subject

Days valid

Cancel

Generate

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

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

gn2.sgws.foo.com.

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

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

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

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

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

12. Klicken Sie Auf **Speichern**.

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

Verwandte Informationen

["Verwalten Sie erhalten"](#)

["Netzwerkrichtlinien"](#)

["Verwalten von Hochverfügbarkeitsgruppen"](#)

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

Bearbeiten von Load Balancer-Endpunkten

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

Was Sie benötigen

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

Schritte

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

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

Endpunkte mit bald auslaufenden Zertifikaten sind in der Tabelle aufgeführt.

Load Balancer Endpoints

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

	Display name	Port	Using HTTPS
<input type="radio"/>	Unsecured Endpoint 5	10444	No
<input checked="" type="radio"/>	Secured Endpoint 1	10443	Yes

Displaying 2 endpoints.

- Wählen Sie den Endpunkt aus, den Sie bearbeiten möchten.
- Klicken Sie auf **Endpunkt bearbeiten**.

Das Dialogfeld Endpunkt bearbeiten wird angezeigt.

Für einen ungesicherten (HTTP) Endpunkt wird nur der Abschnitt Konfiguration des Endpoint Service des Dialogfelds angezeigt. Für einen gesicherten Endpunkt (HTTPS) werden die Abschnitte Endpoint Service Configuration und die Zertifikate des Dialogfelds angezeigt, wie im folgenden Beispiel dargestellt.

Endpoint Service Configuration

Endpoint service type S3 Swift

Certificates

Upload Certificate

Generate Certificate

Server

CA

Certificate metadata

```
Subject DN: /C=CA/ST=British Columbia/O=NetApp, Inc./OU=SGQA/CN=*.mraymond-grid-a.sgqa.eng.netapp.com
Serial Number: 1C:FD:27:8B:E6:A5:BA:30:45:A9:16:4F:DC:77:3E:C6:80:7D:AF:E9
Issuer DN: /C=CA/ST=British Columbia/O=EqualSign, Inc./OU=IT/CN=EqualSign Issuing CA
Issued On: 2000-01-01T00:00:00.000Z
Expires On: 3000-01-01T00:00:00.000Z
SHA-1 Fingerprint: 60:3D:5A:8C:62:C5:B8:49:DC:9A:B3:F7:B9:0B:5B:0E:D2:A2:7E:C7
SHA-256 Fingerprint: AF:75:7F:44:C6:86:A4:84:B2:7D:11:DE:9F:49:D3:F6:2A:7E:D9:4D:2A:1B:8A:0B:B3:7E:23:0F:B3:CB:84:8
9
Alternative Names: DNS:*.mraymond-grid-a.sgqa.eng.netapp.com
DNS:*.99-140-dc1-g1.mraymond-grid-a.sgqa.eng.netapp.com
DNS:*.99-142-dc1-s1.mraymond-grid-a.sgqa.eng.netapp.com
```

Certificate PEM

```
-----BEGIN CERTIFICATE-----
MIIHfDCCBWSgAwIBAgIUHP0ni+a1ujBFqRZP3Hc+xoB9r+kwDQYJKoZIhvcNAQEL
BQAwbjELMAkGA1UEBhMCQ0ExGTAXBgNVBAGMEEJyaXRpc2ggQ29sdWliaWExGDAW
BgNVBAoMD0VxdWFsU2lnbiwgSW5jLjELMAkGA1UECwwCSVQxHTAbBgNVBAMMFVx
dWFsU2lnbiBjc3N1aW5nIENBMCAxDTAwMDEwMDEwMDEwMDEwMDEwMDEwMDEw
MDAwWjB+MQswCQYDVQQGEwJDQTEZMBcGA1UECAwQnJpdG1zaCBDb2x1bWpYTEV
MBMGA1UECgwMTmV0QXBwLmVudG9wCwYDVQQQLDARTR1FBMS4wLWYyLWV0QDQD
Lm1yYX1tb25kLWdyYWQtYS5zZ3FhLmVudG9wCwYDVQRhcHAuY29tLmIiBjANBgkqhkiG
9w0BAQEFAAOCQA8AMIIBCgKCAQEaonUkwwFg/B1U1Y+bIR80MaVJSC+R7Sfz1O2v
Hz4rSnrYCh/WJRCT+fznmxzaGs2RRUDinLnX1Yk+QUPAdIFZ+Sldr6HlrYTP/NK
-----END CERTIFICATE-----
```

- Nehmen Sie die gewünschten Änderungen am Endpunkt vor.

Für einen ungesicherten (HTTP-)Endpunkt können Sie:

- Ändern Sie den Endpunkt-Servicetyp zwischen S3 und Swift.

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

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



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

5. Klicken Sie Auf **Speichern**.

Verwandte Informationen

[Erstellen von Load Balancer-Endpunkten](#)

Entfernen von Load Balancer-Endpunkten

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

Was Sie benötigen

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

Schritte

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

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

Load Balancer Endpoints

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

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

Displaying 2 endpoints.

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

Ein Bestätigungsdialogfeld wird angezeigt.

Warning

Remove Endpoint

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

Cancel

OK

4. Klicken Sie auf **OK**.

Der Endpunkt wird entfernt.

Wie der Lastenausgleich funktioniert - CLB-Service

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

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

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

The screenshot shows the StorageGRID Webconsole interface. On the left, the 'Grid Topology' tree is expanded to show 'Data Center 1' > 'DC1-G1-98-161' > 'CLB'. On the right, the 'Overview Summary - DC1-G1-98-161' page is displayed, showing a 'Storage Capacity' table with the following data:

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

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

Verwandte Informationen

["Was sind Verbindungskosten"](#)

["Verbindungskosten werden aktualisiert"](#)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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