# Referenz für Netzwerk-Ports

StorageGRID

NetApp
April 10, 2024

This PDF was generated from https://docs.netapp.com/de-de/storagegrid-116/network/internal-grid-node-communications.html on April 10, 2024. Always check docs.netapp.com for the latest.

# Inhalt

Referenz für Netzwerk-Ports . . . . . 1
Interne Kommunikation mit Grid-Nodes . . . . . 1
Externe Kommunikation . . . . . 6

# Referenz für Netzwerk-Ports

Sie müssen sicherstellen, dass die Netzwerkinfrastruktur interne und externe Kommunikation zwischen Knoten innerhalb des Grid und externen Clients und Services ermöglicht. Möglicherweise benötigen Sie Zugriff über interne und externe Firewalls, Switching-Systeme und Routing-Systeme.

Verwenden Sie die Details für Interne Kommunikation mit Grid-Nodes Und Externe Kommunikation Um zu bestimmen, wie die einzelnen erforderlichen Ports konfiguriert werden.

## Interne Kommunikation mit Grid-Nodes

Die interne StorageGRID-Firewall erlaubt nur eingehende Verbindungen zu bestimmten Ports im Grid-Netzwerk, mit Ausnahme der Ports 22, 80, 123 und 443 (siehe Informationen zur externen Kommunikation). Verbindungen werden auch an Ports akzeptiert, die durch Load Balancer-Endpunkte definiert wurden.

> NetApp empfiehlt, ICMP (Internet Control Message Protocol)-Datenverkehr zwischen den Grid-Knoten zu aktivieren. Das erlauben von ICMP-Datenverkehr kann die Failover-Performance verbessern, wenn ein Grid-Knoten nicht erreicht werden kann.

Zusätzlich zu ICMP und den in der Tabelle aufgeführten Ports verwendet StorageGRID das Virtual Router Redundancy Protocol (VRRP). VRRP ist ein Internetprotokoll, das IP-Protokoll Nummer 112 verwendet. StorageGRID verwendet VRRP nur im Unicast-Modus. VRRP ist nur erforderlich, wenn Hochverfügbarkeitsgruppen Werden konfiguriert.

### Richtlinien für Linux-basierte Knoten

Wenn Netzwerkrichtlinien des Unternehmens den Zugriff auf einen dieser Ports einschränken, können Sie Ports während der Bereitstellung mithilfe eines Konfigurationsparameters neu zuordnen. Weitere Informationen über die Zuordnung von Ports und die Konfigurationsparameter für die Bereitstellung finden Sie unter:

- Installieren Sie Red hat Enterprise Linux oder CentOS
- Installieren Sie Ubuntu oder Debian

### Richtlinien für VMware-basierte Nodes

Konfigurieren Sie die folgenden Ports nur dann, wenn Sie Firewall-Einschränkungen definieren müssen, die sich außerhalb des VMware-Netzwerks befinden.

Wenn Netzwerkrichtlinien des Unternehmens den Zugriff auf eine dieser Ports einschränken, können Sie bei der Implementierung von Nodes mit dem VMware vSphere Web Client Ports neu zuordnen oder bei der Automatisierung der Grid Node-Bereitstellung eine Konfigurationsdateieinstellung verwenden. Weitere Informationen über die Zuordnung von Ports und die Konfigurationsparameter für die Bereitstellung finden Sie unterVMware installieren.

### Richtlinien für Appliance-Nodes

Wenn Netzwerkrichtlinien des Unternehmens den Zugriff auf eine dieser Ports einschränken, können Sie Ports mithilfe des StorageGRID Appliance Installer neu zuordnen. Weitere Informationen zur Port-Neuzuordnung für

Appliances finden Sie unter:

- SG100- und SG1000-Services-Appliances
- SG6000 Storage-Appliances
- SG5700 Storage-Appliances
- SG5600 Storage Appliances

## Interne StorageGRID-Ports

| Port | TCP oder UDP | Von | Bis | Details |
|---|---|---|---|---|
| 22 | TCP | Primärer Admin-Node | Alle Nodes | Bei Wartungsarbeiten muss der primäre Admin-Node mit SSH am Port 22 mit allen anderen Nodes kommunizieren können. Das Aktivieren von SSH-Datenverkehr von anderen Nodes ist optional. |
| 80 | TCP | Appliances | Primärer Admin-Node | Verwendet von StorageGRID-Appliances, um mit dem primären Admin-Knoten zu kommunizieren, um die Installation zu starten. |
| 123 | UDP | Alle Nodes | Alle Nodes | Netzwerkzeitprotokolldienst. Jeder Node synchronisiert seine Zeit mithilfe von NTP mit jedem anderen Node. |
| 443 | TCP | Alle Nodes | Primärer Admin-Node | Wird zur Kommunikation des Status an den primären Admin-Knoten während der Installation und anderen Wartungsverfahren verwendet. |

| | | | | |
|---|---|---|---|---|
| 1139 | TCP | Storage-Nodes | Storage-Nodes | Interner Datenverkehr zwischen Speicherknoten. |
| 1501 | TCP | Alle Nodes | Storage-Nodes mit ADC | Reporting-, Audit- und Konfigurationsdaten verkehr. |
| 1502 | TCP | Alle Nodes | Storage-Nodes | Interner S3- und Swift-Datenverkehr. |
| 1504 | TCP | Alle Nodes | Admin-Nodes | NMS-Service-Berichterstellung und interner Datenverkehr bei der Konfiguration. |
| 1505 | TCP | Alle Nodes | Admin-Nodes | AMS-Dienst internen Verkehr. |
| 1506 | TCP | Alle Nodes | Alle Nodes | Serverstatus interner Datenverkehr. |
| 1507 | TCP | Alle Nodes | Gateway-Nodes | Interner Datenverkehr des Load Balancer: |
| 1508 | TCP | Alle Nodes | Primärer Admin-Node | Interner Datenverkehr im Konfigurationsmana gement. |
| 1509 | TCP | Alle Nodes | Archiv-Nodes | Interner Datenverkehr des Archivierungs-Knotens. |
| 1511 | TCP | Alle Nodes | Storage-Nodes | Interner Metadaten-Datenverkehr: |

| | | | | |
|---|---|---|---|---|
| 5353 | UDP | Alle Nodes | Alle Nodes | Optional wird er für vollGrid-IP-Änderungen und für die primäre Admin Node-Erkennung während der Installation, Erweiterung und Recovery verwendet. |
| 7001 | TCP | Storage-Nodes | Storage-Nodes | Cassandra TLS zwischen Nodes-Cluster-Kommunikation |
| 7443 | TCP | Alle Nodes | Admin-Nodes | Interner Datenverkehr für Wartungsvorgänge und Fehlerberichte. |
| 8443 | TCP | Primärer Admin-Node | Appliance-Nodes | Interner Datenverkehr im Zusammenhang mit dem Wartungsmodus. |
| 9042 | TCP | Storage-Nodes | Storage-Nodes | Cassandra-Client-Port: |
| 9999 | TCP | Alle Nodes | Alle Nodes | Interner Datenverkehr für mehrere Dienste. Beinhaltet Wartungsvorgänge, Kennzahlen und Netzwerk-Updates. |
| 10226 | TCP | Storage-Nodes | Primärer Admin-Node | Wird von StorageGRID Appliances verwendet, um AutoSupport Meldungen von E-Series SANtricity System Manager an den primären Admin-Node weiterzuleiten. |

| | | | | |
|---|---|---|---|---|
| 11139 | TCP | Archivierung/Storage-Nodes | Archivierung/Storage-Nodes | Interner Datenverkehr zwischen Speicherknoten und Archivknoten. |
| 18000 | TCP | Admin/Storage-Nodes | Storage-Nodes mit ADC | Kontodienst, interner Datenverkehr. |
| 18001 | TCP | Admin/Storage-Nodes | Storage-Nodes mit ADC | Interner Datenverkehr der Identitätsföderation. |
| 18002 | TCP | Admin/Storage-Nodes | Storage-Nodes | Interner API-Traffic im Zusammenhang mit Objektprotokollen. |
| 18003 | TCP | Admin/Storage-Nodes | Storage-Nodes mit ADC | Plattform Dienste internen Traffic. |
| 18017 | TCP | Admin/Storage-Nodes | Storage-Nodes | Interner Datenverkehr des Data Mover-Service für Cloud-Speicherpools. |
| 18019 | TCP | Storage-Nodes | Storage-Nodes | Interner Traffic beim Chunk-Service für Erasure Coding. |
| 18082 | TCP | Admin/Storage-Nodes | Storage-Nodes | Interner S3-Datenverkehr. |
| 18083 | TCP | Alle Nodes | Storage-Nodes | Swift-bezogener interner Traffic: |
| 18200 | TCP | Admin/Storage-Nodes | Storage-Nodes | Weitere Statistiken zu Client-Anforderungen. |
| 19000 | TCP | Admin/Storage-Nodes | Storage-Nodes mit ADC | Keystone-Service: Interner Datenverkehr. |

**Verwandte Informationen**

Externe Kommunikation

# Externe Kommunikation

Die Clients müssen mit den Grid-Nodes kommunizieren, um Inhalte aufzunehmen und abzurufen. Die verwendeten Ports hängen von den ausgewählten Objekt-Storage-Protokollen ab. Diese Ports müssen dem Client zugänglich sein.

## Eingeschränkter Zugriff auf Ports

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf beliebige Ports einschränken, können Sie dies verwenden Load Balancer-Endpunkte Um den Zugriff auf benutzerdefinierte Ports zu erlauben. Sie können dann verwenden Nicht vertrauenswürdige Client-Netzwerke Um den Zugriff nur auf Endpunkt-Ports des Load Balancer zu erlauben.

## Port-Neuzuordnung

Um Systeme und Protokolle wie SMTP, DNS, SSH oder DHCP verwenden zu können, müssen Sie beim Implementieren von Nodes Ports neu zuordnen. Sie sollten jedoch die Load Balancer-Endpunkte nicht neu zuordnen. Informationen zum Ummappen von Ports finden Sie in den Installationsanweisungen für Ihre Plattform:

**Softwarebasierte Nodes**

- Installieren Sie Red hat Enterprise Linux oder CentOS
- Installieren Sie Ubuntu oder Debian
- VMware installieren

**Appliance-Nodes**

- SG100- und SG1000-Services-Appliances
- SG6000 Storage-Appliances
- SG5700 Storage-Appliances
- SG5600 Storage Appliances

## Anschlüsse für externe Kommunikation

In der folgenden Tabelle werden die Ports für den Datenverkehr zu den Nodes aufgeführt.

> Diese Liste enthält keine Ports, die als konfiguriert werden können Load Balancer-Endpunkte Oder verwendet für "Syslog-Server".

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|---|---|---|---|---|---|
| 22 | TCP | SSH | Service-Laptop | Alle Nodes | Für Verfahren mit Konsolenschritten ist ein SSH- oder Konsolenzugriff erforderlich. Optional können Sie statt 22 auch Port 2022 verwenden. |

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|---|---|---|---|---|---|
| 25 | TCP | SMTP | Admin-Nodes | E-Mail-Server | Wird für Warnungen und E-Mail-basierte AutoSupport verwendet. Sie können die Standard-Porteinstellung von 25 über die Seite „E-Mail-Server“ außer Kraft setzen. |
| 53 | TCP/UDP | DNS | Alle Nodes | DNS-Server | Wird für das Domain Name System verwendet. |
| 67 | UDP | DHCP | Alle Nodes | DHCP-Service | Optional zur Unterstützung einer DHCP-basierten Netzwerkkonfiguration. Der dhclient-Dienst wird nicht für statisch konfigurierte Grids ausgeführt. |
| 68 | UDP | DHCP | DHCP-Service | Alle Nodes | Optional zur Unterstützung einer DHCP-basierten Netzwerkkonfiguration. Der dhclient-Dienst wird nicht für Raster ausgeführt, die statische IP-Adressen verwenden. |
| 80 | TCP | HTTP | Browser | Admin-Nodes | Port 80 wird für die Admin-Node-Benutzeroberfläche an Port 443 umgeleitet. |
| 80 | TCP | HTTP | Browser | Appliances | Port 80 wird für das Installationsprogramm der StorageGRID-Appliance an Port 8443 umgeleitet. |
| 80 | TCP | HTTP | Storage-Nodes mit ADC | AWS | Wird für Plattform-Services-Meldungen verwendet, die an AWS oder andere externe Services gesendet werden, die HTTP verwenden. Mandanten können bei der Erstellung eines Endpunkts die Standard-HTTP-Porteinstellung von 80 außer Kraft setzen. |

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|---|---|---|---|---|---|
| 80 | TCP | HTTP | Storage-Nodes | AWS | An AWS Ziele mit HTTP gesendete Anfragen von Cloud-Storage-Pools Grid-Administratoren können die Standard-HTTP-Port-Einstellung von 80 bei der Konfiguration eines Cloud-Storage-Pools außer Kraft setzen. |
| 111 | TCP/UDP | Rpcbind | NFS Client | Admin-Nodes | Wird vom NFS-basierten Audit-Export verwendet (Portmap).<br><br>**Hinweis:** dieser Port ist nur erforderlich, wenn der NFS-basierte Audit-Export aktiviert ist. |
| 123 | UDP | NTP | Primäre NTP-Knoten | Externe NTP | Netzwerkzeitprotokolldienst. Als primäre NTP-Quellen ausgewählte Nodes synchronisieren auch die Uhrzeiten mit den externen NTP-Zeitquellen. |
| 137 | UDP | NetBIOS | SMB-Client | Admin-Nodes | Wird vom SMB-basierten Audit-Export für Clients verwendet, die NetBIOS-Unterstützung benötigen.<br><br>**Hinweis:** dieser Port ist nur erforderlich, wenn der SMB-basierte Audit-Export aktiviert ist. |
| 138 | UDP | NetBIOS | SMB-Client | Admin-Nodes | Wird vom SMB-basierten Audit-Export für Clients verwendet, die NetBIOS-Unterstützung benötigen.<br><br>**Hinweis:** dieser Port ist nur erforderlich, wenn der SMB-basierte Audit-Export aktiviert ist. |

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|---|---|---|---|---|---|
| 139 | TCP | SMB | SMB-Client | Admin-Nodes | Wird vom SMB-basierten Audit-Export für Clients verwendet, die NetBIOS-Unterstützung benötigen.<br><br>**Hinweis:** dieser Port ist nur erforderlich, wenn der SMB-basierte Audit-Export aktiviert ist. |
| 161 | TCP/UDP | SNMP | SNMP-Client | Alle Nodes | Wird für SNMP-Abfrage verwendet. Alle Knoten stellen grundlegende Informationen zur Verfügung; Admin Nodes stellen auch Alarm- und Alarmdaten zur Verfügung. Standardmäßig auf UDP-Port 161 gesetzt, wenn konfiguriert.<br><br>**Hinweis:** dieser Port ist nur erforderlich und wird nur auf der Knoten-Firewall geöffnet, wenn SNMP konfiguriert ist. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren.<br><br>**Hinweis:** um Informationen zur Verwendung von SNMP mit StorageGRID zu erhalten, wenden Sie sich an Ihren NetApp Ansprechpartner. |

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|---|---|---|---|---|---|
| 162 | TCP/UDP | SNMP-Benachrichtigungen | Alle Nodes | Benachrichtigungsziele | Ausgehende SNMP-Benachrichtigungen und Traps standardmäßig auf UDP-Port 162.<br><br>**Hinweis:** dieser Port ist nur erforderlich, wenn SNMP aktiviert ist und Benachrichtigungsziele konfiguriert sind. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren.<br><br>**Hinweis:** um Informationen zur Verwendung von SNMP mit StorageGRID zu erhalten, wenden Sie sich an Ihren NetApp Ansprechpartner. |
| 389 | TCP/UDP | LDAP | Storage-Nodes mit ADC | Active Directory/LDAP | Wird zur Verbindung mit einem Active Directory- oder LDAP-Server für Identity Federation verwendet. |
| 443 | TCP | HTTPS | Browser | Admin-Nodes | Wird von Webbrowsern und Management-API-Clients für den Zugriff auf Grid Manager und Tenant Manager verwendet. |
| 443 | TCP | HTTPS | Admin-Nodes | Active Directory | Wird von Admin-Nodes verwendet, die eine Verbindung zu Active Directory herstellen, wenn Single Sign-On (SSO) aktiviert ist. |
| 443 | TCP | HTTPS | Archiv-Nodes | Amazon S3 | Wird für den Zugriff von Archiv-Nodes auf Amazon S3 verwendet. |

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|---|---|---|---|---|---|
| 443 | TCP | HTTPS | Storage-Nodes mit ADC | AWS | Wird für Plattform-Services-Nachrichten verwendet, die an AWS oder andere externe Services gesendet werden, die HTTPS verwenden. Mandanten können bei der Erstellung eines Endpunkts die Standard-HTTP-Porteinstellung von 443 außer Kraft setzen. |
| 443 | TCP | HTTPS | Storage-Nodes | AWS | Cloud-Storage-Pools-Anfragen werden an AWS-Ziele mit HTTPS gesendet. Grid-Administratoren können die HTTPS-Porteinstellung von 443 bei der Konfiguration eines Cloud-Storage-Pools außer Kraft setzen. |
| 445 | TCP | SMB | SMB-Client | Admin-Nodes | Wird vom SMB-basierten Audit-Export verwendet.<br><br>**Hinweis:** dieser Port ist nur erforderlich, wenn der SMB-basierte Audit-Export aktiviert ist. |
| 903 | TCP | NFS | NFS Client | Admin-Nodes | Wird vom NFS-basierten Audit-Export verwendet (`rpc.mountd`).<br><br>**Hinweis:** dieser Port ist nur erforderlich, wenn der NFS-basierte Audit-Export aktiviert ist. |
| 2022 | TCP | SSH | Service-Laptop | Alle Nodes | Für Verfahren mit Konsolenschritten ist ein SSH- oder Konsolenzugriff erforderlich. Optional können Sie statt 2022 auch Port 22 verwenden. |

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|---|---|---|---|---|---|
| 2049 | TCP | NFS | NFS Client | Admin-Nodes | Wird vom NFS-basierten Audit-Export verwendet (nfs).<br><br>**Hinweis:** dieser Port ist nur erforderlich, wenn der NFS-basierte Audit-Export aktiviert ist. |
| 5696 | TCP | KMIP | Appliance | KMS | KMIP (Key Management Interoperability Protocol): Externer Datenverkehr von Appliances, die für die Node-Verschlüsselung auf den Verschlüsselungsmanagemen t-Server (Key Management Interoperability Protocol) konfiguriert sind, es sei denn, ein anderer Port wird auf der KMS-Konfigurationsseite des StorageGRID Appliance Installer angegeben. |
| 8022 | TCP | SSH | Service-Laptop | Alle Nodes | SSH auf Port 8022 gewährt Zugriff auf das Betriebssystem auf Appliance- und virtuellen Node-Plattformen zur Unterstützung und Fehlerbehebung. Dieser Port wird nicht für Linux-basierte (Bare Metal-)Nodes verwendet und muss nicht zwischen Grid-Nodes oder während des normalen Betriebs zugänglich sein. |
| 8082 | TCP | HTTPS | S3-Clients | Gateway-Nodes | S3-Client-Traffic zum veralteten CLB-Dienst auf Gateway-Nodes (HTTPS). |
| 8083 | TCP | HTTPS | Swift Clients | Gateway-Nodes | Schneller Client-Datenverkehr zum veralteten CLB-Dienst auf Gateway-Nodes (HTTPS). |
| 8084 | TCP | HTTP | S3-Clients | Gateway-Nodes | S3-Client-Traffic zum veralteten CLB-Dienst auf Gateway-Nodes (HTTP). |

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|---|---|---|---|---|---|
| 8085 | TCP | HTTP | Swift Clients | Gateway-Nodes | Schneller Client-Datenverkehr zum veralteten CLB-Dienst auf Gateway Nodes (HTTP). |
| 8443 | TCP | HTTPS | Browser | Admin-Nodes | Optional Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Grid Manager verwendet. Kann zur Trennung der Kommunikation zwischen Grid Manager und Tenant Manager verwendet werden. |
| 9022 | TCP | SSH | Service-Laptop | Appliances | Gewährt Zugriff auf StorageGRID Appliances im Vorkonfigurationsmodus für Support und Fehlerbehebung. Dieser Port muss während des normalen Betriebs nicht zwischen Grid-Nodes oder auf diesen zugreifen können. |
| 9091 | TCP | HTTPS | Externer Grafana-Service | Admin-Nodes | Wird von externen Grafana Services für sicheren Zugriff auf den StorageGRID Prometheus Service verwendet.<br><br>**Hinweis:** dieser Port wird nur benötigt, wenn der zertifikatbasierte Prometheus-Zugriff aktiviert ist. |
| 9443 | TCP | HTTPS | Browser | Admin-Nodes | Optional Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Mandanten-Manager verwendet. Kann zur Trennung der Kommunikation zwischen Grid Manager und Tenant Manager verwendet werden. |
| 18082 | TCP | HTTPS | S3-Clients | Storage-Nodes | S3-Client-Datenverkehr direkt zu Storage-Nodes (HTTPS). |

| Port | TCP oder UDP | Protokoll | Von | Bis | Details |
|---|---|---|---|---|---|
| 18083 | TCP | HTTPS | Swift Clients | Storage-Nodes | Schneller Client-Verkehr direkt zu Storage Nodes (HTTPS). |
| 18084 | TCP | HTTP | S3-Clients | Storage-Nodes | S3-Client-Traffic direkt zu Storage-Nodes (HTTP). |
| 18085 | TCP | HTTP | Swift Clients | Storage-Nodes | Schneller Client-Verkehr direkt zu Storage Nodes (HTTP). |

**Copyright-Informationen**

Copyright © 2024 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.