



# Referenz für Netzwerk-Ports

StorageGRID software

NetApp  
February 12, 2026

# Inhalt

- Referenz für Netzwerk-Ports ..... 1
  - Interne Grid-Knotenkommunikation für StorageGRID ..... 1
    - Richtlinien für Linux-basierte Knoten ..... 1
    - Richtlinien für VMware-basierte Nodes ..... 1
    - Richtlinien für Appliance-Nodes ..... 1
    - Interne StorageGRID-Ports ..... 2
  - Externe Kommunikation für StorageGRID ..... 4
    - Eingeschränkter Zugriff auf Ports ..... 5
    - Anschlüsse für externe Kommunikation ..... 5

# Referenz für Netzwerk-Ports

## Interne Grid-Knotenkommunikation für StorageGRID

Die interne StorageGRID Firewall ermöglicht eingehende Verbindungen zu bestimmten Ports im Grid-Netzwerk. 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. Wenn ICMP-Datenverkehr zugelassen wird, kann die Failover-Performance verbessert werden, 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"](#) konfiguriert sind.

### Richtlinien für Linux-basierte Knoten

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf diese Ports einschränken, können Sie die Ports zum Zeitpunkt der Bereitstellung mithilfe eines Bereitstellungsconfigurationsparameters neu zuordnen. Weitere Informationen zur Portneuordnung und zu den Bereitstellungsconfigurationsparametern finden Sie unter ["Installieren Sie StorageGRID auf softwarebasierten Knoten"](#).



Die Unterstützung für die Neuordnung von Ports ist veraltet und wird in einer zukünftigen Version entfernt. Informationen zum Entfernen neu zugeordneter Ports finden Sie unter ["Entfernen Sie die Port-Remaps auf Bare-Metal-Hosts"](#).

### 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 die Netzwerkrichtlinien des Unternehmens den Zugriff auf diese Ports einschränken, können Sie die Ports neu zuordnen, wenn Sie Knoten mithilfe des VMware vSphere Web Client bereitstellen oder indem Sie bei der Automatisierung der Grid-Knotenbereitstellung eine Konfigurationsdateieinstellung verwenden. Weitere Informationen zur Port-Neuordnung und zu den Konfigurationsparametern für die Bereitstellung finden Sie in den Anweisungen für ["Installieren von StorageGRID auf VMware"](#).



Die Unterstützung für die Neuordnung von Ports ist veraltet und wird in einer zukünftigen Version entfernt. Informationen zum Entfernen neu zugeordneter Ports finden Sie unter ["Entfernen Sie die Port-Remaps auf Bare-Metal-Hosts"](#).

### 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. Siehe ["Optional: Netzwerkports für Appliance neu zuordnen"](#).



Die Unterstützung für die Neuordnung von Ports ist veraltet und wird in einer zukünftigen Version entfernt. Informationen zum Entfernen neu zugeordneter Ports finden Sie unter ["Entfernen Sie Port-Neuzuordnungen auf StorageGRID -Geräten"](#) .

## 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.
1055	TCP	Alle Nodes	Primärer Admin-Node	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.
1139	TCP	Storage-Nodes	Storage-Nodes	Interner Datenverkehr zwischen Speicherknoten.
1501	TCP	Alle Nodes	Storage-Nodes mit ADC	Reporting-, Audit- und Konfigurationsdatenverkehr.
1502	TCP	Alle Nodes	Storage-Nodes	Interner S3-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.

Port	TCP oder UDP	Von	Bis	Details
1507	TCP	Alle Nodes	Gateway-Nodes	Interner Datenverkehr des Load Balancer:
1508	TCP	Alle Nodes	Primärer Admin-Node	Interner Datenverkehr im Konfigurationsmanagement.
1511	TCP	Alle Nodes	Storage-Nodes	Interner Metadaten-Datenverkehr:
5353	UDP	Alle Nodes	Alle Nodes	<p>Stellt den Multicast-DNS-Dienst (mDNS) bereit, der für Full-Grid-IP-Änderungen und für die Erkennung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird.</p> <p><b>Hinweis:</b> Die Konfiguration dieses Ports ist optional.</p>
7001	TCP	Storage-Nodes	Storage-Nodes	Cassandra TLS zwischen Nodes-Cluster-Kommunikation
7443	TCP	Alle Nodes	Primärer Admin-Node	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung, andere Wartungsverfahren und Fehlerberichterstattung.
8011	TCP	Alle Nodes	Primärer Admin-Node	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.
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 für die Weiterleitung von AutoSupport-Paketen vom E-Series SANtricity System Manager zum primären Admin-Node verwendet.
10342	TCP	Alle Nodes	Primärer Admin-Node	Interner Datenverkehr für Installations-, Erweiterungs-, Wiederherstellungs- und andere Wartungsverfahren.

Port	TCP oder UDP	Von	Bis	Details
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	Alle Nodes	Alle Nodes	Interner Datenverkehr des Chunk-Dienstes für Erasure Coding und Replikation
18082	TCP	Admin/Storage-Nodes	Storage-Nodes	Interner S3-Datenverkehr.
18086	TCP	Alle Nodes	Storage-Nodes	Interner Datenverkehr im Zusammenhang mit dem LDR-Dienst.
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 für StorageGRID

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 einen der Ports einschränken, können Sie einen der folgenden Schritte ausführen:

- Mit ["Load Balancer-Endpunkte"](#) können Sie den Zugriff auf benutzerdefinierte Ports zulassen.
- Weisen Sie bei der Implementierung von Nodes Ports neu zu. Sie sollten jedoch die Load Balancer-Endpunkte nicht neu zuordnen. Weitere Informationen zur Port-Neuzuweisung für den StorageGRID-Node finden Sie unter:



Die Unterstützung für die Neuordnung von Ports ist veraltet und wird in einer zukünftigen Version entfernt. Informationen zum Entfernen neu zugeordneter Ports finden Sie unter ["Entfernen Sie Port-Neuzuordnungen auf StorageGRID -Geräten"](#) oder ["Entfernen Sie die Port-Remaps auf Bare-Metal-Hosts"](#).

- ["Port-Neuzuordnungsschlüssel für StorageGRID auf Red hat Enterprise Linux"](#)
- ["Ports für StorageGRID auf VMware neu zuordnen"](#)
- ["Optional: Netzwerkports für Appliance neu zuordnen"](#)

## Anschlüsse für externe Kommunikation

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



Diese Liste enthält keine Ports, die möglicherweise als konfiguriert werden ["Load Balancer-Endpunkte"](#).

Port	TCP oder UDP	Protokoll	Von	Bis	Details
22	TCP	SSH	Service-Laptop	Alle Nodes	Für Verfahren mit Konsolenschritten ist SSH- oder Konsolenzugriff erforderlich. Optional können Sie Port 2022 anstelle von 22 verwenden.  <b>Hinweis:</b> Dieser Port wird nur benötigt, wenn Sie den SSH-Zugriff für bestimmte Wartungsarbeiten aktivieren müssen.
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 DNS 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.

Port	TCP oder UDP	Protokoll	Von	Bis	Details
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-Nachrichten verwendet, die an AWS oder andere externe Services gesendet werden, die HTTP verwenden. Mandanten können beim Erstellen eines Endpunkts die Standard-HTTP-Porteinstellung 80 außer Kraft setzen.
80	TCP	HTTP	Storage-Nodes	AWS	Cloud-Storage-Pools-Anfragen werden an AWS-Ziele mit HTTP gesendet. Grid-Administratoren können die HTTP-Porteinstellung von 80 bei der Konfiguration eines Cloud-Storage-Pools außer Kraft setzen.
123	UDP	NTP	Primäre NTP-Knoten	Externe NTP	Netzwerkzeitprotokolldienst. Als primäre NTP-Quellen ausgewählte Nodes synchronisieren auch die Uhrzeiten mit den externen NTP-Zeitquellen.
161	TCP/UDP	SNMP	SNMP-Client	Alle Nodes	<p>Wird für SNMP-Abfrage verwendet. Alle Nodes bieten grundlegende Informationen, Admin-Nodes stellen auch Warnungsdaten bereit. Standardmäßig auf UDP-Port 161 gesetzt, wenn konfiguriert.</p> <p><b>Hinweis:</b> 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.</p> <p><b>Hinweis:</b> um Informationen zur Verwendung von SNMP mit StorageGRID zu erhalten, wenden Sie sich an Ihren NetApp Ansprechpartner.</p>



Port	TCP oder UDP	Protokoll	Von	Bis	Details
162	TCP/UDP	SNMP-Benachrichtigungen	Alle Nodes	Benachrichtigungsziele	<p>Ausgehende SNMP-Benachrichtigungen und Traps standardmäßig auf UDP-Port 162.</p> <p><b>Hinweis:</b> dieser Port ist nur erforderlich, wenn SNMP aktiviert ist und Benachrichtigungsziele konfiguriert sind. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren.</p> <p><b>Hinweis:</b> um Informationen zur Verwendung von SNMP mit StorageGRID zu erhalten, wenden Sie sich an Ihren NetApp Ansprechpartner.</p>
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	<p>Wird von Webbrowsern und Management-API-Clients verwendet, um auf den Grid Manager und den Tenant Manager zuzugreifen.</p> <p><b>Hinweis:</b> Wenn Sie die Grid Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit über einen blockierten Port verbunden sind (einschließlich Ihnen), den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde zur Liste der privilegierten Adressen hinzugefügt. Siehe "<a href="#">Konfigurieren Sie die Firewall-Steuerelemente</a>" um privilegierte IP-Adressen zu konfigurieren.</p>
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	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 beim Erstellen eines Endpunkts die Standard-HTTP-Porteinstellung 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.

Port	TCP oder UDP	Protokoll	Von	Bis	Details
5353	UDP	MDNS	Alle Nodes	Alle Nodes	<p>Stellt den Multicast-DNS-Dienst (mDNS) bereit, der für Full-Grid-IP-Änderungen und für die Erkennung des primären Admin-Knotens während der Installation, Erweiterung und Wiederherstellung verwendet wird.</p> <p><b>Hinweis:</b> Die Konfiguration dieses Ports ist optional.</p>
5696	TCP	KMIP	Appliance	KMS	<p>KMIP (Key Management Interoperability Protocol): Externer Datenverkehr von Appliances, die für die Node-Verschlüsselung auf den Verschlüsselungsmanagement-Server (Key Management Interoperability Protocol) konfiguriert sind, es sei denn, ein anderer Port wird auf der KMS-Konfigurationsseite des StorageGRID Appliance Installer angegeben.</p>
8443	TCP	HTTPS	Browser	Admin-Nodes	<p>Optional. Wird von Webbrowsern und Management-API-Clients für den Zugriff auf den Grid Manager verwendet. Kann verwendet werden, um die Kommunikation zwischen Grid Manager und Tenant Manager zu trennen.</p> <p><b>Hinweis:</b> Wenn Sie die Grid Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit über einen blockierten Port verbunden sind (einschließlich Ihnen), den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde zur Liste der privilegierten Adressen hinzugefügt. Siehe "<a href="#">Konfigurieren Sie die Firewall-Steuerelemente</a>" um privilegierte IP-Adressen zu konfigurieren.</p>
8443	TCP	HTTPS	Browser	Appliances	<p>Wird von Webbrowsern und Verwaltungs-API-Clients verwendet, um auf das StorageGRID Appliance Installer zuzugreifen.</p> <p><b>Hinweis:</b> Port 443 leitet für den StorageGRID Appliance Installer auf Port 8443 um.</p>
9022	TCP	SSH	Service-Laptop	Appliances	<p>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.</p>

Port	TCP oder UDP	Protokoll	Von	Bis	Details
9091	TCP	HTTPS	Externer Grafana-Service	Admin-Nodes	<p>Wird von externen Grafana Services für sicheren Zugriff auf den StorageGRID Prometheus Service verwendet.</p> <p><b>Hinweis:</b> dieser Port wird nur benötigt, wenn der zertifikatbasierte Prometheus-Zugriff aktiviert ist.</p>
9092	TCP	Kafka	Storage-Nodes mit ADC	Kafka-Cluster	Wird für Meldungen über Plattformdienste verwendet, die an ein Kafka-Cluster gesendet werden. Mandanten können beim Erstellen eines Endpunkts die Standard-Kafka-Porteinstellung 9092 außer Kraft setzen.
9443	TCP	HTTPS	Browser	Admin-Nodes	Optional. Wird von Webbrowsern und Verwaltungs-API-Clients für den Zugriff auf den Tenant Manager verwendet. Kann verwendet werden, um die Kommunikation zwischen Grid Manager und Tenant Manager zu trennen.
18082	TCP	HTTPS	S3-Clients	Storage-Nodes	S3-Client-Traffic direkt zu Storage-Nodes (HTTPS).
18084	TCP	HTTP	S3-Clients	Storage-Nodes	S3-Client-Traffic direkt zu Storage-Nodes (HTTP).
23000-23999	TCP	HTTPS	Alle Nodes im Quell-Grid für die Grid-übergreifende Replizierung	Admin Nodes und Gateway Nodes im Ziel-Grid für Grid-übergreifende Replizierung	Dieser Port-Bereich ist für Grid Federation-Verbindungen reserviert. Beide Grids in einer bestimmten Verbindung verwenden den gleichen Port.

## Copyright-Informationen

Copyright © 2026 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.