



Netzwerkportreferenz

StorageGRID software

NetApp

November 04, 2025

Inhalt

Netzwerkportreferenz	1
Interne Grid-Knoten-Kommunikation	1
Richtlinien für Linux-basierte Knoten	1
Richtlinien für VMware-basierte Knoten	1
Richtlinien für Appliance-Knoten	1
Interne StorageGRID Ports	1
Externe Kommunikation	4
Eingeschränkter Zugang zu Häfen	5
Für die externe Kommunikation verwendete Ports	5

Netzwerkportreferenz

Interne Grid-Knoten-Kommunikation

Die interne Firewall von StorageGRID ermöglicht eingehende Verbindungen zu bestimmten Ports im Grid-Netzwerk. Verbindungen werden auch auf Ports akzeptiert, die von Load Balancer-Endpunkten definiert werden.



NetApp empfiehlt, den ICMP-Verkehr (Internet Control Message Protocol) zwischen Grid-Knoten zu aktivieren. Das Zulassen von ICMP-Verkehr kann die Failover-Leistung 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 die IP-Protokollnummer 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 Bereitstellungskonfigurationsparameters neu zuordnen. Weitere Informationen zur Portneuzuordnung und zu den Bereitstellungskonfigurationsparametern finden Sie unter:

- "[Installieren Sie StorageGRID unter Red Hat Enterprise Linux](#)"
- "[Installieren Sie StorageGRID unter Ubuntu oder Debian](#)"

Richtlinien für VMware-basierte Knoten

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

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 Portneuzuordnung und zu den Bereitstellungskonfigurationsparametern finden Sie unter "[Installieren Sie StorageGRID auf VMware](#)".

Richtlinien für Appliance-Knoten

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf diese Ports einschränken, können Sie die Ports mithilfe des StorageGRID Appliance Installer neu zuordnen. Sehen "[Optional: Netzwerkports für das Gerät neu zuordnen](#)".

Interne StorageGRID Ports

Hafen	TCP oder UDP	Aus	Zu	Details
22	TCP	Primärer Admin-Knoten	Alle Knoten	Für Wartungsverfahren muss der primäre Admin-Knoten in der Lage sein, über SSH auf Port 22 mit allen anderen Knoten zu kommunizieren. Das Zulassen von SSH-Verkehr von anderen Knoten ist optional.
80	TCP	Geräte	Primärer Admin-Knoten	Wird von StorageGRID -Geräten verwendet, um mit dem primären Admin-Knoten zu kommunizieren und die Installation zu starten.
123	UDP	Alle Knoten	Alle Knoten	Netzwerkzeitprotokolldienst. Jeder Knoten synchronisiert seine Zeit mit jedem anderen Knoten über NTP.
443	TCP	Alle Knoten	Primärer Admin-Knoten	Wird verwendet, um während der Installation und anderer Wartungsvorgänge den Status an den primären Admin-Knoten zu übermitteln.
1055	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung und andere Wartungsverfahren.
1139	TCP	Speicherknoten	Speicherknoten	Interner Datenverkehr zwischen Speicherknoten.
1501	TCP	Alle Knoten	Speicherknoten mit ADC	Berichterstellung, Prüfung und Konfiguration des internen Datenverkehrs.
1502	TCP	Alle Knoten	Speicherknoten	S3- und Swift-bezogener interner Datenverkehr.
1504	TCP	Alle Knoten	Admin-Knoten	NMS-Dienstberichterstattung und Konfiguration des internen Datenverkehrs.
1505	TCP	Alle Knoten	Admin-Knoten	AMS-Service-interner Verkehr.
1506	TCP	Alle Knoten	Alle Knoten	Serverstatus interner Datenverkehr.
1507	TCP	Alle Knoten	Gateway-Knoten	Interner Datenverkehr des Load Balancers.
1508	TCP	Alle Knoten	Primärer Admin-Knoten	Interner Datenverkehr des Konfigurationsmanagements.

Hafen	TCP oder UDP	Aus	Zu	Details
1511	TCP	Alle Knoten	Speicherkn oten	Metadaten des internen Datenverkehrs.
5353	UDP	Alle Knoten	Alle Knoten	<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>Hinweis: Die Konfiguration dieses Ports ist optional.</p>
7001	TCP	Speicherkn oten	Speicherkn oten	Cassandra TLS-Clusterkommunikation zwischen Knoten.
7443	TCP	Alle Knoten	Primärer Admin- Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung, andere Wartungsverfahren und Fehlerberichterstattung.
8011	TCP	Alle Knoten	Primärer Admin- Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung und andere Wartungsverfahren.
8443	TCP	Primärer Admin- Knoten	Appliance- Knoten	Interner Verkehr im Zusammenhang mit dem Wartungsmodusverfahren.
9042	TCP	Speicherkn oten	Speicherkn oten	Cassandra-Client-Port.
9999	TCP	Alle Knoten	Alle Knoten	Interner Datenverkehr für mehrere Dienste. Beinhaltet Wartungsverfahren, Metriken und Netzwerkupdates.
10226	TCP	Speicherkn oten	Primärer Admin- Knoten	Wird von StorageGRID -Geräten zum Weiterleiten von AutoSupport Paketen vom E-Series SANtricity System Manager an den primären Admin-Knoten verwendet.
10342	TCP	Alle Knoten	Primärer Admin- Knoten	Interner Datenverkehr für Installation, Erweiterung, Wiederherstellung und andere Wartungsverfahren.
18000	TCP	Admin-/Speicherkn oten	Speicherkn oten mit ADC	Interner Datenverkehr des Kontodienstes.

Hafen	TCP oder UDP	Aus	Zu	Details
18001	TCP	Admin-/Speicherknöten	Speicherknöten mit ADC	Interner Datenverkehr der Identity Federation.
18002	TCP	Admin-/Speicherknöten	Speicherknöten	Interner API-Verkehr im Zusammenhang mit Objektprotokollen.
18003	TCP	Admin-/Speicherknöten	Speicherknöten mit ADC	Die Plattform bedient den internen Datenverkehr.
18017	TCP	Admin-/Speicherknöten	Speicherknöten	Interner Datenverkehr des Data Mover-Dienstes für Cloud Storage Pools.
18019	TCP	Alle Knoten	Alle Knoten	Interner Datenverkehr des Chunk-Dienstes für Erasure Coding und Replikation
18082	TCP	Admin-/Speicherknöten	Speicherknöten	S3-bezogener interner Datenverkehr.
18083	TCP	Alle Knoten	Speicherknöten	Swift-bezogener interner Verkehr.
18086	TCP	Alle Knoten	Speicherknöten	Interner Verkehr im Zusammenhang mit dem LDR-Dienst.
18200	TCP	Admin-/Speicherknöten	Speicherknöten	Zusätzliche Statistiken zu Clientanfragen.
19000	TCP	Admin-/Speicherknöten	Speicherknöten mit ADC	Interner Verkehr des Keystone -Dienstes.

Ähnliche Informationen

["Externe Kommunikation"](#)

Externe Kommunikation

Clients müssen mit Grid-Knoten kommunizieren, um Inhalte aufzunehmen und abzurufen. Die verwendeten Ports hängen von den gewählten Objektspeicherprotokollen ab. Diese Ports müssen für den Client zugänglich sein.

Eingeschränkter Zugang zu Häfen

Wenn die Netzwerkrichtlinien des Unternehmens den Zugriff auf einen der Ports einschränken, können Sie Folgendes tun:

- Verwenden "[Load Balancer-Endpunkte](#)" um den Zugriff auf benutzerdefinierte Ports zu ermöglichen.
- Ordnen Sie die Ports beim Bereitstellen von Knoten neu zu. Sie sollten die Endpunkte des Lastenausgleichs jedoch nicht neu zuordnen. Sehen Sie sich die Informationen zur Portneuzuordnung für Ihren StorageGRID Knoten an:
 - "[Port-Neuzuordnungsschlüssel für StorageGRID unter Red Hat Enterprise Linux](#)"
 - "[Port-Neuzuordnungsschlüssel für StorageGRID unter Ubuntu oder Debian](#)"
 - "[Ports für StorageGRID auf VMware neu zuordnen](#)"
 - "[Optional: Netzwerkports für das Gerät neu zuordnen](#)"

Für die externe Kommunikation verwendete Ports

Die folgende Tabelle zeigt die für den Datenverkehr in die Knoten verwendeten Ports.



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

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
22	TCP	SSH	Service-Laptop	Alle Knoten	Für Verfahren mit Konsolenschritten ist SSH- oder Konsolenzugriff erforderlich. Optional können Sie Port 2022 anstelle von 22 verwenden.
25	TCP	SMTP	Admin-Knoten	E-Mail-Server	Wird für Warnungen und E-Mail-basierten AutoSupport verwendet. Sie können die Standard-Porteinstellung von 25 auf der Seite „E-Mail-Server“ überschreiben.
53	TCP/UDP	DNS	Alle Knoten	DNS-Server	Wird für DNS verwendet.
67	UDP	DHCP	Alle Knoten	DHCP-Dienst	Wird optional zur Unterstützung der DHCP-basierten Netzwerkkonfiguration verwendet. Der dhclient-Dienst wird für statisch konfigurierte Grids nicht ausgeführt.
68	UDP	DHCP	DHCP-Dienst	Alle Knoten	Wird optional zur Unterstützung der DHCP-basierten Netzwerkkonfiguration verwendet. Der dhclient-Dienst wird nicht für Grids ausgeführt, die statische IP-Adressen verwenden.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
80	TCP	HTTP	Browser	Admin-Knoten	Port 80 leitet für die Benutzeroberfläche des Admin-Knotens auf Port 443 um.
80	TCP	HTTP	Browser	Geräte	Port 80 leitet für den StorageGRID Appliance Installer auf Port 8443 um.
80	TCP	HTTP	Speicher-Knoten mit ADC	AWS	Wird für Plattformdienstnachrichten verwendet, die an AWS oder andere externe Dienste gesendet werden, die HTTP verwenden. Mandanten können die Standard-HTTP-Porteinstellung von 80 beim Erstellen eines Endpunkts überschreiben.
80	TCP	HTTP	Speicher-Knoten	AWS	An AWS-Ziele gesendete Cloud Storage Pools-Anfragen, die HTTP verwenden. Grid-Administratoren können die Standard-HTTP-Porteinstellung von 80 beim Konfigurieren eines Cloud-Speicherpools überschreiben.
111	TCP/UDP	RPCBind	NFS-Client	Admin-Knoten	<p>Wird vom NFS-basierten Audit-Export (Portmap) verwendet.</p> <p>Hinweis: Dieser Port wird nur benötigt, wenn der NFS-basierte Audit-Export aktiviert ist.</p> <p>Hinweis: Die Unterstützung für NFS ist veraltet und wird in einer zukünftigen Version entfernt.</p>
123	UDP	NTP	Primäre NTP-Knoten	Externes NTP	Netzwerkzeitprotokolldienst. Als primäre NTP-Quellen ausgewählte Knoten synchronisieren auch die Uhrzeiten mit den externen NTP-Zeitquellen.
161	TCP/UDP	SNMP	SNMP-Client	Alle Knoten	<p>Wird für SNMP-Polling verwendet. Alle Knoten stellen grundlegende Informationen bereit; Admin-Knoten stellen auch Warndaten bereit. Bei Konfiguration wird standardmäßig der UDP-Port 161 verwendet.</p> <p>Hinweis: Dieser Port ist nur erforderlich und wird nur in der Knoten-Firewall geöffnet, wenn SNMP konfiguriert ist. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren.</p> <p>Hinweis: Informationen zur Verwendung von SNMP mit StorageGRID erhalten Sie von Ihrem NetApp Kundenbetreuer.</p>

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
162	TCP/UDP	SNMP-Benachrichtigungen	Alle Knoten	Benachrichtigungsziele	<p>Ausgehende SNMP-Benachrichtigungen und Traps werden standardmäßig an UDP-Port 162 gesendet.</p> <p>Hinweis: Dieser Port ist nur erforderlich, wenn SNMP aktiviert und Benachrichtigungsziele konfiguriert sind. Wenn Sie SNMP verwenden möchten, können Sie alternative Ports konfigurieren.</p> <p>Hinweis: Informationen zur Verwendung von SNMP mit StorageGRID erhalten Sie von Ihrem NetApp Kundenbetreuer.</p>
389	TCP/UDP	LDAP	Speichergeräten mit ADC	Active Directory/LDAP	Wird zum Herstellen einer Verbindung mit einem Active Directory- oder LDAP-Server für die Identitätsföderation verwendet.
443	TCP	HTTPS	Browser	Admin-Knoten	<p>Wird von Webbrowsersn und Management-API-Clients verwendet, um auf den Grid Manager und den Tenant Manager zuzugreifen.</p> <p>Hinweis: 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 "Konfigurieren der Firewall-Steuerelemente" um privilegierte IP-Adressen zu konfigurieren.</p>
443	TCP	HTTPS	Admin-Knoten	Active Directory	Wird von Admin-Knoten verwendet, die eine Verbindung zu Active Directory herstellen, wenn Single Sign-On (SSO) aktiviert ist.
443	TCP	HTTPS	Speichergeräten mit ADC	AWS	Wird für Plattformdienstnachrichten verwendet, die an AWS oder andere externe Dienste gesendet werden, die HTTPS verwenden. Mandanten können die Standard-HTTP-Porteinstellung 443 beim Erstellen eines Endpunkts überschreiben.
443	TCP	HTTPS	Speichergeräten	AWS	An AWS-Ziele gesendete Cloud Storage Pools-Anfragen, die HTTPS verwenden. Grid-Administratoren können die Standard-HTTPS-Porteinstellung 443 beim Konfigurieren eines Cloud-Speicherpools überschreiben.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
903	TCP	NFS	NFS-Client	Admin-Knoten	<p>Wird vom NFS-basierten Audit-Export verwendet(<code>rpc.mountd</code>).</p> <p>Hinweis: Dieser Port wird nur benötigt, wenn der NFS-basierte Audit-Export aktiviert ist.</p> <p>Hinweis: Die Unterstützung für NFS ist veraltet und wird in einer zukünftigen Version entfernt.</p>
2022	TCP	SSH	Service-Laptop	Alle Knoten	<p>Für Verfahren mit Konsolenschritten ist SSH- oder Konsolenzugriff erforderlich. Optional können Sie Port 22 anstelle von 2022 verwenden.</p>
2049	TCP	NFS	NFS-Client	Admin-Knoten	<p>Wird vom NFS-basierten Audit-Export (NFS) verwendet.</p> <p>Hinweis: Dieser Port wird nur benötigt, wenn der NFS-basierte Audit-Export aktiviert ist.</p> <p>Hinweis: Die Unterstützung für NFS ist veraltet und wird in einer zukünftigen Version entfernt.</p>
5353	UDP	mDNS	Alle Knoten	Alle Knoten	<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>Hinweis: Die Konfiguration dieses Ports ist optional.</p>
5696	TCP	KMIP	Gerät	KMS	<p>Externer Datenverkehr des Key Management Interoperability Protocol (KMIP) von für die Knotenverschlüsselung konfigurierten Geräten zum Key Management Server (KMS), sofern auf der KMS-Konfigurationsseite des StorageGRID Appliance Installer kein anderer Port angegeben ist.</p>
8022	TCP	SSH	Service-Laptop	Alle Knoten	<p>SSH auf Port 8022 gewährt Zugriff auf das Basisbetriebssystem auf Appliance- und virtuellen Knotenplattformen für Support und Fehlerbehebung. Dieser Port wird nicht für Linux-basierte (Bare-Metal-)Knoten verwendet und muss zwischen Grid-Knoten oder während des normalen Betriebs nicht zugänglich sein.</p>

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
8443	TCP	HTTPS	Browser	Admin-Knoten	<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>Hinweis: 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 "Konfigurieren der Firewall-Steuerelemente" um privilegierte IP-Adressen zu konfigurieren.</p>
8443	TCP	HTTPS	Browser	Geräte	<p>Wird von Webbrowsern und Verwaltungs-API-Clients verwendet, um auf das StorageGRID Appliance Installer zuzugreifen.</p> <p>Hinweis: Port 443 leitet für den StorageGRID Appliance Installer auf Port 8443 um.</p>
9022	TCP	SSH	Service-Laptop	Geräte	Gewährt Zugriff auf StorageGRID -Geräte im Vorkonfigurationsmodus für Support und Fehlerbehebung. Dieser Port muss zwischen Grid-Knoten oder während des normalen Betriebs nicht zugänglich sein.
9091	TCP	HTTPS	Externer Grafana-Dienst	Admin-Knoten	<p>Wird von externen Grafana-Diensten für den sicheren Zugriff auf den StorageGRID Prometheus-Dienst verwendet.</p> <p>Hinweis: Dieser Port wird nur benötigt, wenn der zertifikatsbasierte Prometheus-Zugriff aktiviert ist.</p>
9092	TCP	Kafka	Speicher-Knoten mit ADC	Kafka-Cluster	Wird für Plattformdienstnachrichten verwendet, die an einen Kafka-Cluster gesendet werden. Mandanten können die standardmäßige Kafka-Porteinstellung von 9092 beim Erstellen eines Endpunkts überschreiben.
9443	TCP	HTTPS	Browser	Admin-Knoten	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.

Hafen	TCP oder UDP	Protokoll	Aus	Zu	Details
18082	TCP	HTTPS	S3-Clients	Speicherknoten	S3-Client-Verkehr direkt zu Speicherknoten (HTTPS).
18083	TCP	HTTPS	Swift-Clients	Speicherknoten	Swift-Client-Verkehr direkt zu Speicherknoten (HTTPS).
18084	TCP	HTTP	S3-Clients	Speicherknoten	S3-Client-Verkehr direkt zu Speicherknoten (HTTP).
18085	TCP	HTTP	Swift-Clients	Speicherknoten	Swift-Client-Verkehr direkt zu Speicherknoten (HTTP).
23000-23999	TCP	HTTPS	Alle Knoten im Quellgrid für die Cross-Grid-Replikation	Admin-Knoten und Gateway-Knoten im Ziel-Grid für die Cross-Grid-Replikation	Dieser Portbereich ist für Grid-Föderation-Verbindungen reserviert. Beide Grids in einer bestimmten Verbindung verwenden denselben Port.

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 BESCHRÄNKKT 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 BESCHRÄNKKT 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 IRGENDERWEINER 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.