



So implementiert StorageGRID die S3- REST-API

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

- So implementiert StorageGRID die S3-REST-API 1
- In Konflikt stehende Clientanforderungen 1
- Konsistenzkontrollen 1
- Managen von Objekten durch StorageGRID ILM-Regeln 4
- Objektversionierung 6
- Empfehlungen für die Implementierung der S3-REST-API 7

So implementiert StorageGRID die S3-REST-API

Eine Client-Applikation kann S3-REST-API-Aufrufe zur Verbindung mit StorageGRID nutzen, um Buckets zu erstellen, zu löschen und zu ändern sowie Objekte zu speichern und abzurufen.

- ["In Konflikt stehende Clientanforderungen"](#)
- ["Konsistenzkontrollen"](#)
- ["Managen von Objekten durch StorageGRID ILM-Regeln"](#)
- ["Objektversionierung"](#)
- ["Empfehlungen für die Implementierung der S3-REST-API"](#)

In Konflikt stehende Clientanforderungen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „latest-WINS“-Basis gelöst.

Der Zeitpunkt für die Auswertung „latest-WINS“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf, wenn S3-Clients einen Vorgang starten.

Konsistenzkontrollen

Konsistenzkontrollen ermöglichen je nach Anforderung einen Kompromiss zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Storage-Nodes und -Standorte.

Standardmäßig garantiert StorageGRID eine Lese-/Nachher-Konsistenz für neu erstellte Objekte. Jeder GET nach einem erfolgreich abgeschlossenen PUT wird in der Lage sein, die neu geschriebenen Daten zu lesen. Überschreibungen vorhandener Objekte, Metadatenaktualisierungen und -Löschungen sind schließlich konsistent. Überschreibungen dauern in der Regel nur wenige Sekunden oder Minuten, können jedoch bis zu 15 Tage in Anspruch nehmen.

Wenn Sie Objektvorgänge auf einer anderen Konsistenzstufe ausführen möchten, können Sie für jeden Bucket oder für jeden API-Vorgang eine Konsistenzkontrolle angeben.

Konsistenzkontrollen

Die Konsistenzkontrolle beeinflusst die Verteilung der Metadaten, die StorageGRID zum Verfolgen von Objekten zwischen Nodes verwendet, und somit die Verfügbarkeit von Objekten für Client-Anforderungen.

Sie können die Konsistenzkontrolle für einen Bucket- oder API-Vorgang auf einen der folgenden Werte festlegen:

Konsistenzkontrolle	Beschreibung
Alle	Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.

Konsistenzkontrolle	Beschreibung
Stark global	Garantierte Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen an allen Standorten.
Stark vor Ort	Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.
Read-after-New-Write-Funktion	<p>(Standard) konsistente Lese-/Schreibvorgänge für neue Objekte und eventuelle Konsistenz bei Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung Entspricht den Amazon S3 -Konsistenzgarantien.</p> <p>Hinweis: Wenn Ihre Anwendung HEAD Requests für Objekte verwendet, die nicht vorhanden sind, erhalten Sie möglicherweise eine hohe Anzahl von 500 internen Serverfehlern, wenn ein oder mehrere Speicherknoten nicht verfügbar sind. Um diese Fehler zu vermeiden, setzen Sie das Consistency Control auf „available“, es sei denn, Sie benötigen Konsistenzgarantien ähnlich wie Amazon S3.</p>
Verfügbar (eventuelle Konsistenz für DEN HAUPTBETRIEB)	Verhält sich wie die Konsistenzstufe „read-after-New-write“, bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB. Bietet höhere Verfügbarkeit FÜR HEAD-Operationen als „read-after-New-write“, wenn Storage Nodes nicht verfügbar sind. Unterschied zu Amazon S3 Konsistenzgarantien nur für HEAD-Operationen.

Verwenden der Consistency Controls „read-after-New-write“ und „available“

Wenn ein KOPF- oder GET-Vorgang die Konsistenzkontrolle „read-after-New-write“ verwendet oder EIN GET-Vorgang die Konsistenzkontrolle „available“ verwendet, führt StorageGRID die Suche in mehreren Schritten durch:

- Es sieht zunächst das Objekt mit einer niedrigen Konsistenz.
- Falls dieses Lookup fehlschlägt, wird das Lookup auf der nächsten Konsistenzebene wiederholt, bis es die höchste Konsistenzstufe „all,“ erreicht, sodass alle Kopien der Objektmetadaten verfügbar sein müssen.

Wenn ein KOPF- oder GET-Vorgang die Konsistenzkontrolle „read-after-New-write“ verwendet, aber das Objekt nicht vorhanden ist, erreicht die Objekt-Lookup immer die Konsistenzstufe „all“. Da auf dieser Konsistenzstufe alle Kopien der Objektmetadaten verfügbar sein müssen, können Sie eine hohe Anzahl von 500 Fehlern des internen Servers erhalten, wenn ein oder mehrere Storage-Nodes nicht verfügbar sind.

Sofern Sie keine Konsistenzgarantien wie Amazon S3 benötigen, können Sie diese Fehler bei DEN HEAD-Operationen vermeiden, indem Sie die Consistency Control auf „available“ setzen. Wenn ein

HAUPTBETRIEB die Konsistenzkontrolle „Available“ verwendet, bietet StorageGRID eventuell nur Konsistenz. Ein fehlgeschlagener Vorgang wird erst wieder versucht, wenn es die Konsistenzstufe „all“ erreicht. Daher müssen nicht alle Kopien der Objektmetadaten verfügbar sein.

Angeben der Consistency Control für einen API-Vorgang

Um die Consistency Control für einen einzelnen API-Vorgang festzulegen, müssen für den Vorgang Konsistenzkontrollen unterstützt werden, und Sie müssen die Consistency Control in der Anforderungs-Kopfzeile angeben. In diesem Beispiel wird die Consistency Control auf „strong-site“ für EINE GET Object Operation gesetzt.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: <em>authorization name</em>
Host: <em>host</em>
Consistency-Control: strong-site
```



Sie müssen für DEN PUT-Objekt- und DEN GET-Objektbetrieb dasselbe Konsistenzsteuerelement verwenden.

Angeben der Konsistenzkontrolle für einen Bucket

Zum Festlegen der Konsistenzkontrolle für Bucket können Sie die StorageGRID PUT Bucket-Konsistenzanforderung und DIE ANFORDERUNG FÜR GET-Bucket-Konsistenz verwenden. Alternativ können Sie den Tenant Manager oder die Mandantenmanagement-API verwenden.

Beachten Sie beim Festlegen der Konsistenzkontrollen für einen Bucket Folgendes:

- Durch das Festlegen der Konsistenzkontrolle für einen Bucket wird festgelegt, welche Konsistenzkontrolle für S3-Operationen verwendet wird, die für Objekte im Bucket oder in der Bucket-Konfiguration durchgeführt werden. Er hat keine Auswirkungen auf die Vorgänge auf dem Bucket selbst.
- Die Konsistenzkontrolle für einen einzelnen API-Vorgang überschreibt die Konsistenzkontrolle für den Bucket.
- Im Allgemeinen sollte für Buckets die standardmäßige Konsistenzkontrolle verwendet werden, „read-after-New-write.“ Wenn Anforderungen nicht korrekt funktionieren, ändern Sie das Verhalten des Anwendungs-Clients, wenn möglich. Oder konfigurieren Sie den Client so, dass für jede API-Anforderung das Consistency Control angegeben wird. Legen Sie die Consistency Control auf Bucket-Ebene nur als letztes Resort fest.

Konsistenzkontrollen und ILM-Regeln interagieren, um die Datensicherung zu beeinträchtigen

Die Wahl der Konsistenzkontrolle und der ILM-Regel haben Auswirkungen auf den Schutz von Objekten. Diese Einstellungen können interagieren.

Die beim Speichern eines Objekts verwendete Konsistenzkontrolle beeinflusst beispielsweise die anfängliche Platzierung von Objekt-Metadaten, während das für die ILM-Regel ausgewählte Aufnahmeverhalten sich auf die anfängliche Platzierung von Objektkopien auswirkt. Da StorageGRID Zugriff auf die Metadaten eines Objekts und seine Daten benötigt, um Kundenanforderungen zu erfüllen, kann die Auswahl der passenden Sicherungsstufen für Konsistenz und Aufnahme-Verhalten eine bessere Erstsicherung und zuverlässigere

Systemantworten ermöglichen.

Die folgenden Aufnahmeverhalten stehen für ILM-Regeln zur Verfügung:

- **Streng:** Alle in der ILM-Regel angegebenen Kopien müssen erstellt werden, bevor der Erfolg an den Client zurückgesendet wird.
- **Ausgewogen:** StorageGRID versucht bei der Aufnahme alle in der ILM-Regel festgelegten Kopien zu erstellen; wenn dies nicht möglich ist, werden Zwischenkopien erstellt und der Erfolg an den Client zurückgesendet. Die Kopien, die in der ILM-Regel angegeben sind, werden, wenn möglich gemacht.
- **Dual Commit:** StorageGRID erstellt sofort Zwischenkopien des Objekts und gibt den Erfolg an den Kunden zurück. Kopien, die in der ILM-Regel angegeben sind, werden nach Möglichkeit erstellt.



Lesen Sie vor der Auswahl des Aufnahmeverhaltens für eine ILM-Regel die vollständige Beschreibung dieser Einstellungen in den Anweisungen zum Managen von Objekten mit Information Lifecycle Management.

Beispiel für die Interaktion zwischen Konsistenzkontrolle und ILM-Regel

Angenommen, Sie haben ein Grid mit zwei Standorten mit der folgenden ILM-Regel und der folgenden Einstellung für die Konsistenzstufe:

- **ILM-Regel:** Erstellen Sie zwei Objektkopien, eine am lokalen Standort und eine an einem entfernten Standort. Das strikte Aufnahmeverhalten wird ausgewählt.
- **Konsistenzstufe:** „strong-global“ (Objektmetadaten werden sofort auf alle Standorte verteilt.)

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID sowohl Objektkopien als auch verteilt Metadaten an beiden Standorten, bevor der Kunde zum Erfolg zurückkehrt.

Das Objekt ist zum Zeitpunkt der Aufnahme der Nachricht vollständig gegen Verlust geschützt. Wenn beispielsweise der lokale Standort kurz nach der Aufnahme verloren geht, befinden sich Kopien der Objektdaten und der Objektmetadaten am Remote-Standort weiterhin. Das Objekt kann vollständig abgerufen werden.

Falls Sie stattdessen dieselbe ILM-Regel und die Konsistenzstufe „strong-site“ verwendet haben, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem Objektdaten an den Remote-Standort repliziert wurden, doch bevor die Objektmetadaten dort verteilt werden. In diesem Fall entspricht die Sicherung von Objektmetadaten nicht dem Schutzniveau für Objektdaten. Falls der lokale Standort kurz nach der Aufnahme verloren geht, gehen Objektmetadaten verloren. Das Objekt kann nicht abgerufen werden.

Die Wechselbeziehung zwischen Konsistenzstufen und ILM-Regeln kann komplex sein. Wenden Sie sich an NetApp, wenn Sie Hilfe benötigen.

Verwandte Informationen

["Objektmanagement mit ILM"](#)

["Get Bucket-Konsistenzanforderung"](#)

["PUT Bucket-Konsistenzanforderung"](#)

Managen von Objekten durch StorageGRID ILM-Regeln

Der Grid-Administrator erstellt Informationen Lifecycle Management (ILM)-Regeln für das

Management von Objektdaten, die von S3-REST-API-Client-Applikationen in das StorageGRID-System aufgenommen werden. Diese Regeln werden dann zur ILM-Richtlinie hinzugefügt, um zu bestimmen, wie und wo Objektdaten im Laufe der Zeit gespeichert werden.

ILM-Einstellungen bestimmen die folgenden Aspekte eines Objekts:

- **Geographie**

Der Speicherort der Objektdaten kann entweder im StorageGRID-System (Storage-Pool) oder in einem Cloud-Storage-Pool gespeichert werden.

- * Speicherklasse*

Storage-Typ zur Speicherung von Objektdaten, z. B. Flash oder rotierende Festplatte

- **Verlustschutz**

Wie viele Kopien erstellt werden und welche Arten von Kopien erstellt werden: Replizierung, Erasure Coding oder beides.

- **Aufbewahrung**

Es ändert sich im Laufe der Zeit, wie Objektdaten verwaltet werden, wo sie gespeichert sind und wie sie vor Verlust geschützt sind.

- **Schutz während der Aufnahme**

Methode zum Schutz von Objektdaten bei der Aufnahme: Synchrone Platzierung (mit ausgeglichenen oder strengen Optionen für das Aufnahmeverhalten) oder Erstellung von vorläufigen Kopien (unter Verwendung der Option Dual-Commit)

ILM-Regeln können Objekte filtern und auswählen. Bei mit S3 aufgenommenen Objekten können ILM-Regeln Objekte auf Basis der folgenden Metadaten filtern:

- Mandantenkonto
- Bucket-Name
- Aufnahmezeit
- Taste
- Zeitpunkt Des Letzten Zugriffs



Standardmäßig werden Updates der letzten Zugriffszeit für alle S3 Buckets deaktiviert. Wenn Ihr StorageGRID System eine ILM-Regel enthält, die die Option „Last Access Time“ verwendet, müssen Sie für die in dieser Regel angegebenen S3-Buckets Updates für die letzte Zugriffszeit aktivieren. Sie können Updates der letzten Zugriffszeit mithilfe der Anforderung PUT Bucket Last Access Time, des Checkbox **S3 > Buckets > Letzter Zugriffszeitpunkt konfigurieren** im Tenant Manager oder mithilfe der Tenant Management API aktivieren. Beachten Sie bei der Aktivierung von Updates der letzten Zugriffszeit, dass die Performance von StorageGRID möglicherweise reduziert wird, insbesondere bei Systemen mit kleinen Objekten.

- Speicherortbeschränkung
- Objektgröße
- Benutzermetadaten
- Objekt-Tag

Weitere Informationen zum ILM finden Sie in den Anweisungen zum Managen von Objekten mit Information Lifecycle Management.

Verwandte Informationen

["Verwenden Sie ein Mandantenkonto"](#)

["Objektmanagement mit ILM"](#)

["PUT Anforderung der Uhrzeit des letzten Bucket-Zugriffs"](#)

Objektversionierung

Sie können mithilfe der Versionierung mehrere Versionen eines Objekts aufbewahren, das vor versehentlichem Löschen von Objekten schützt und Ihnen das Abrufen und Wiederherstellen älterer Versionen eines Objekts ermöglicht.

Das StorageGRID System implementiert Versionierung mit Unterstützung für die meisten Funktionen und weist einige Einschränkungen auf. StorageGRID unterstützt bis zu 1,000 Versionen jedes Objekts.

Die Objektversionierung kann mit StorageGRID Information Lifecycle Management (ILM) oder mit der S3 Bucket Lifecycle-Konfiguration kombiniert werden. Sie müssen für jeden Bucket die Versionierung aktivieren, um diese Funktion für den Bucket zu aktivieren. Jedem Objekt im Bucket wird eine Version-ID zugewiesen, die vom StorageGRID-System generiert wird.

Die Verwendung von MFA (Multi-Faktor-Authentifizierung) Löschen wird nicht unterstützt.



Die Versionierung kann nur auf Buckets aktiviert werden, die mit StorageGRID Version 10.3 oder höher erstellt wurden.

ILM und Versionierung

ILM-Richtlinien werden auf jede Version eines Objekts angewendet. Ein ILM-Scanprozess scannt kontinuierlich alle Objekte und bewertet sie anhand der aktuellen ILM-Richtlinie neu. Alle Änderungen, die Sie an ILM-Richtlinien vornehmen, werden auf alle zuvor aufgenommenen Objekte angewendet. Dies umfasst bereits aufgenommene Versionen, wenn die Versionierung aktiviert ist. Beim ILM-Scannen werden neue ILM-Änderungen an zuvor aufgenommenen Objekten angewendet.

Bei S3-Objekten in mit Versionierung aktivierten Buckets können Sie mithilfe der Versionierung ILM-Regeln erstellen, die nicht aktuelle Zeit als Referenzzeit verwenden. Wenn ein Objekt aktualisiert wird, werden seine vorherigen Versionen nicht aktuell. Mithilfe eines nicht aktuellen Zeitfilters können Sie Richtlinien erstellen, die die Auswirkungen früherer Objektversionen auf den Storage verringern.



Wenn Sie eine neue Version eines Objekts über einen mehrteiligen Upload-Vorgang hochladen, wird der nicht aktuelle Zeitpunkt für die Originalversion des Objekts angezeigt, wenn der mehrteilige Upload für die neue Version erstellt wurde, nicht erst nach Abschluss des mehrteiligen Uploads. In begrenzten Fällen kann die nicht aktuelle Zeit der ursprünglichen Version Stunden oder Tage früher als die Zeit für die aktuelle Version sein.

Anweisungen zum Managen von Objekten mit Information Lifecycle Management finden Sie in den Anweisungen, wie z. B. eine ILM-Richtlinie für versionierte Objekte mit S3 enthält.

Verwandte Informationen

["Objektmanagement mit ILM"](#)

Empfehlungen für die Implementierung der S3-REST-API

Bei der Implementierung der S3-REST-API zur Verwendung mit StorageGRID sollten Sie diese Empfehlungen beachten.

Empfehlungen für Köpfe zu nicht vorhandenen Objekten

Wenn Ihre Anwendung regelmäßig prüft, ob ein Objekt in einem Pfad existiert, in dem Sie nicht erwarten, dass das Objekt tatsächlich vorhanden ist, sollten Sie die Konsistenzkontrolle „available“ verwenden. Verwenden Sie zum Beispiel die Konsistenzkontrolle „Available“, wenn Ihre Anwendung einen Speicherort vor DEM ANSETZEN an sie leitet.

Andernfalls werden möglicherweise 500 Fehler des internen Servers angezeigt, wenn ein oder mehrere Speicherknoten nicht verfügbar sind.

Sie können die Konsistenzkontrolle „Available“ für jeden Bucket mithilfe der PUT Bucket-Konsistenzanforderung festlegen oder Sie können die Konsistenzkontrolle in der Anforderungs-Kopfzeile für einen einzelnen API-Vorgang festlegen.

Empfehlungen für Objektschlüssel

Bei Buckets, die in StorageGRID 11.4 oder höher erstellt wurden, ist es nicht mehr erforderlich, Objektschlüsselnamen auf die Performance-Best-Practices zu beschränken. Sie können jetzt beispielsweise Zufallswerte für die ersten vier Zeichen von Objektschlüsselnamen verwenden.

Befolgen Sie bei Buckets, die in Versionen vor StorageGRID 11.4 erstellt wurden, weiterhin die folgenden Empfehlungen für Objektschlüsselnamen:

- Als die ersten vier Zeichen von Objektschlüsseln sollten Sie keine Zufallswerte verwenden. Dies steht im Gegensatz zu der früheren AWS Empfehlung für wichtige Präfixe. Stattdessen sollten Sie nicht-zufällige, nicht-eindeutige Präfixe verwenden, wie z. B. `image`.
- Wenn Sie die frühere Empfehlung von AWS befolgen, zufällige und eindeutige Zeichen in Schlüsselpräfixen zu verwenden, sollten Sie die Objektschlüssel mit einem Verzeichnisnamen vorschreiben. Verwenden Sie dieses Format:

```
mybucket/mydir/f8e3-image3132.jpg
```

Anstelle dieses Formats:

mybucket/f8e3-image3132.jpg

Empfehlungen für „Range reads“

Wenn die Option **komprimiere gespeicherte Objekte** ausgewählt ist (**Konfiguration > Grid-Optionen**), sollten S3-Client-Anwendungen verhindern, DASS GET-Objekt-Operationen ausgeführt werden, die einen Bereich von Bytes angeben. Diese Vorgänge „range Read“ sind ineffizient, da StorageGRID die Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zugreifen zu können. GET-Objektvorgänge, die einen kleinen Byte-Bereich von einem sehr großen Objekt anfordern, sind besonders ineffizient, beispielsweise ist es sehr ineffizient, einen Bereich von 10 MB von einem komprimierten 50-GB-Objekt zu lesen.

Wenn Bereiche von komprimierten Objekten gelesen werden, können Client-Anforderungen eine Zeitdauer haben.



Wenn Sie Objekte komprimieren müssen und Ihre Client-Applikation Bereichslesevorgänge verwenden muss, erhöhen Sie die Zeitüberschreitung beim Lesen der Anwendung.

Verwandte Informationen

["Konsistenzkontrollen"](#)

["PUT Bucket-Konsistenzanforderung"](#)

["StorageGRID verwalten"](#)

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.