



Überwachungsmeldungen und der Lebenszyklus von Objekten

StorageGRID 11.7

NetApp
April 12, 2024

Inhalt

- Überwachungsmeldungen und der Lebenszyklus von Objekten 1
 - Wann werden Audit-Meldungen generiert? 1
 - Objektaufnahme von Transaktionen 1
 - Löschen von Objekttransaktionen 4
 - Abrufen von Objekttransaktionen 5
 - Nachrichten zum Metadatenupdate 7

Überwachungsmeldungen und der Lebenszyklus von Objekten

Wann werden Audit-Meldungen generiert?

Audit-Nachrichten werden bei jeder Aufnahme, jedem Abruf oder jedem Löschen eines Objekts generiert. Sie können diese Transaktionen im Audit-Protokoll identifizieren, indem Sie API-spezifische (S3 oder Swift) Audit-Nachrichten suchen.

Überwachungsmeldungen werden durch Kennungen verknüpft, die für jedes Protokoll spezifisch sind.

Protokoll	Codieren
Verknüpfen von S3-Vorgängen	S3BK (Eimer), S3KY (Schlüssel) oder beide
Swift-Vorgänge verknüpfen	WCON (Container), WOBJ (Object) oder beides
Verknüpfen interner Vorgänge	CBID (interne Kennung des Objekts)

Timing von Audit-Meldungen

Aufgrund von Faktoren wie Zeitunterschieden zwischen Grid-Nodes, Objektgröße und Netzwerkverzögerungen kann die Reihenfolge der durch die verschiedenen Services erzeugten Audit-Meldungen von den Beispielen in diesem Abschnitt abweichen.

Archiv-Nodes

Die Reihe von Meldungen, die beim Senden von Objektdaten an ein externes Archiv-Speichersystem generiert werden, ist ähnlich wie bei Storage-Nodes, es sei denn, es gibt keine SCMT-Meldung (Store Object Commit). Und die ATCE (Archive Object Store Begin) und ASCE (Archive Object Store End) Nachrichten werden für jede archivierte Kopie von Objektdaten generiert.

Die Reihe von Audit-Meldungen, die beim Abrufen von Objektdaten aus einem externen Archiv-Storage-System generiert werden, ähnelt der für Storage-Nodes, jedoch werden für jede abgerufene Kopie von Objektdaten ARCB (Archivobjekt Retrieve Begin) und ARCE (Archive Object Retrieve End) Nachrichten generiert.

Die beim Löschen von Objektdaten aus einem externen Archivspeichersystem generierte Reihe von Überwachungsmeldungen ähnelt der für Speicherknotten, es sei denn, ES gibt keine SREM (Object Store Remove)-Nachricht und für jede Löschanforderung gibt es eine AREM-Nachricht (Archive Object Remove).

Objektaufnahme von Transaktionen

Sie können Transaktionen zur Client-Aufnahme im Prüfprotokoll identifizieren, indem API-spezifische (S3 oder Swift) Audit-Nachrichten loktiert werden.

In den folgenden Tabellen sind nicht alle während einer Aufnahmetransaktion generierten Audit-Meldungen aufgeführt. Es sind nur die Nachrichten enthalten, die für die Aufzeichnung der Transaktion erforderlich sind.

S3 Aufnahme von Audit-Nachrichten

Codieren	Name	Beschreibung	Verfolgen	Siehe
SPUT	S3 PUT-Transaktion	Eine S3-PUT-Aufnahmerate wurde erfolgreich abgeschlossen.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Objektregeln Erfüllt	Die ILM-Richtlinie wurde für dieses Objekt erfüllt.	CBID	"ORLM: Objektregeln erfüllt"

Swift Ingest-Audit-Nachrichten

Codieren	Name	Beschreibung	Verfolgen	Siehe
WPUT	Swift PUT-Transaktion	EINE Swift PUT-Aufnahme-Transaktion wurde erfolgreich abgeschlossen.	CBID, WCON, WOBJ	"WPUT: Schnell AUSGEDRÜCKT"
ORLM	Objektregeln Erfüllt	Die ILM-Richtlinie wurde für dieses Objekt erfüllt.	CBID	"ORLM: Objektregeln erfüllt"

Beispiel: S3-Objektaufnahme

Die folgende Serie von Audit-Meldungen ist ein Beispiel für die im Revisionsprotokoll generierten und gespeicherten Audit-Meldungen, wenn ein S3-Client ein Objekt in einen Storage-Node (LDR-Service) einspeist.

In diesem Beispiel umfasst die aktive ILM-Richtlinie die ILM-Regel „2 Kopien erstellen“.



Im folgenden Beispiel sind nicht alle während einer Transaktion generierten Audit-Meldungen aufgeführt. Es werden nur solche aufgeführt, die sich auf die S3-Aufnahmetransaktion (SPUT) beziehen.

In diesem Beispiel wird vorausgesetzt, dass zuvor ein S3-Bucket erstellt wurde.

SPUT: S3 PUT

Die SPUT-Meldung gibt an, dass eine S3-PUT-Transaktion ausgegeben wurde, um ein Objekt in einem bestimmten Bucket zu erstellen.

2017-07-

```
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CSTR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:identity:70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SBAC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-3"][CBID(UI64):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM(UI64):150032627859669][ATYP(FC32):SPUT][ANID(UI32):12086324][AMID(FC32):S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: Objektregeln erfüllt

Die ORLM-Meldung gibt an, dass die ILM-Richtlinie für dieses Objekt erfüllt wurde. Die Meldung enthält die CBID des Objekts und den Namen der verwendeten ILM-Regel.

Bei replizierten Objekten umfasst das Feld LOCS die LDR-Node-ID und Volume-ID der Objektstandorte.

2019-07-

```
17T21:18:31.230669[AUDT:[CBID(UI64):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make 2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543 2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

Für Objekte, die mit Erasure Coding codiert wurden, enthält das Feld LOCS die Profil-ID für Erasure Coding und die Gruppen-ID für Erasure Coding

2019-02-23T01:52:54.647537

```
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32):DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[ATYP(FC32):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):4168559046473725560]]
```

Das PFADFELD umfasst S3-Bucket und wichtige Informationen sowie Swift-Container- und Objektinformationen, je nachdem, welche API verwendet wurde.

```

2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]

```

Löschen von Objekttransaktionen

Sie können Transaktionen zum Löschen von Objekten im Prüfprotokoll identifizieren, indem API-spezifische (S3 und Swift) Audit-Meldungen angezeigt werden.

In den folgenden Tabellen sind nicht alle während einer Löschtransaktion generierten Überwachungsmeldungen aufgeführt. Es werden nur Nachrichten enthalten, die zum Verfolgen der Löschtransaktion erforderlich sind.

S3-Audit-Nachrichten löschen

Codieren	Name	Beschreibung	Verfolgen	Siehe
SDEL	S3 Löschen	Anforderung zum Löschen des Objekts aus einem Bucket gemacht.	CBID, S3KY	"SDEL: S3 LÖSCHEN"

Swift Audit-Nachrichten löschen

Codieren	Name	Beschreibung	Verfolgen	Siehe
WDEL	Swift Löschen	Anforderung gemacht, das Objekt aus einem Container oder Container zu löschen.	CBID, WOBJ	"WDEL: Swift LÖSCHEN"

Beispiel: S3-Objektlöschung

Wenn ein S3-Client ein Objekt aus einem Storage-Node (LDR-Service) löscht, wird eine Überwachungsmeldung generiert und im Revisionsprotokoll gespeichert.



Im folgenden Beispiel sind nicht alle während einer Löschtransaktion generierten Audit-Meldungen aufgeführt. Es werden nur diejenigen aufgelistet, die mit der S3-Löschtransaktion (SDEL) in Verbindung stehen.

SDEL: S3 Löschen

Die Objektlöschung beginnt, wenn der Client eine LÖSCHANFORDERUNG an einen LDR-Dienst sendet. Die Meldung enthält den Bucket, aus dem das Objekt gelöscht werden soll, und den S3-Schlüssel des Objekts, der zur Identifizierung des Objekts verwendet wird.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHya1RU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity:70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\CSTR\):"example"\\[S3KY\CSTR\):"testobject-0-
7"\][CBID(UI64):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP(FC32):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]
```

Abrufen von Objekttransaktionen

Sie können Transaktionen zum Abrufen von Objekten im Audit-Protokoll identifizieren, indem API-spezifische (S3 und Swift) Audit-Nachrichten loktiert werden.

In den folgenden Tabellen sind nicht alle während einer Abruftransaktion generierten Überwachungsmeldungen aufgeführt. Es werden nur Nachrichten enthalten, die für die Rückrufs-Transaktion erforderlich sind.

S3-Abruf von Audit-Meldungen

Codieren	Name	Beschreibung	Verfolgen	Siehe
SGET	S3 ABRUFEN	Anforderung zum Abrufen eines Objekts aus einem Bucket	CBID, S3BK, S3KY	"SGET S3 ABRUFEN"

Schnelles Abrufen von Audit-Meldungen

Codieren	Name	Beschreibung	Verfolgen	Siehe
WGET	Swift GET	Anforderung gemacht, ein Objekt aus einem Container abzurufen.	CBID, WCON, WOBJ	"WGET: Schneller ERHALTEN"

Beispiel: S3-Objektabruf

Wenn ein S3-Client ein Objekt von einem Storage-Node (LDR-Service) abrufen, wird eine Audit-Meldung erzeugt und im Revisionsprotokoll gespeichert.

Beachten Sie, dass nicht alle während einer Transaktion generierten Audit-Meldungen im folgenden Beispiel aufgeführt sind. Es werden nur diejenigen aufgelistet, die sich auf die S3-Abruftransaktion (SGET) beziehen.

SGET S3 ABRUFEN

Der Objektabruf beginnt, wenn der Client eine GET Object-Anforderung an einen LDR-Service sendet. Die Meldung enthält den Bucket, aus dem das Objekt abgerufen werden soll, und den S3-Schlüssel des Objekts, der zur Identifizierung des Objekts verwendet wird.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKht7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\CSTR\):"bucket-
anonymous"\]\[S3KY\CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Wenn die Bucket-Richtlinie ermöglicht, kann ein Client Objekte anonym abrufen oder Objekte aus einem Bucket abrufen, der einem anderen Mandantenkonto gehört. Die Überwachungsmeldung enthält Informationen über das Mandantenkonto des Bucket-Inhabers, sodass Sie diese anonymen und Cross-Account-Anforderungen verfolgen können.

In der folgenden Beispielnachricht sendet der Client eine GET Object-Anforderung für ein in einem Bucket gespeichertes Objekt, das nicht Eigentümer ist. Die Werte für SBAI und SBAC zeichnen die Konto-ID und den Namen des Mandanten des Bucket-Besitzers auf. Diese Werte unterscheiden sich von der Konto-ID und dem Namen des in S3AI und SACC aufgezeichneten Clients.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\CSTR\):"17915054115450519830"\]\[SACC\CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\CSTR\):"4397929817
8977966408"\]\[SBAC\CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Beispiel: S3 Select auf einem Objekt

Wenn ein S3-Client eine S3-Select-Abfrage für ein Objekt ausgibt, werden Audit-Meldungen erzeugt und im Revisionsprotokoll gespeichert.

Beachten Sie, dass nicht alle während einer Transaktion generierten Audit-Meldungen im folgenden Beispiel aufgeführt sind. Es werden nur diejenigen aufgelistet, die sich auf die S3 Select-Transaktion (SelectObjectContent) beziehen.

Jede Abfrage ergibt zwei Überwachungsmeldungen: Eine, die die Autorisierung der S3 Select-Anforderung

ausführt (das S3SR-Feld ist auf "select" gesetzt) und eine nachfolgende Standard-GET-Operation, die die Daten während der Verarbeitung aus dem Speicher abrufen.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAIP(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-05064f74126d"][S3KY(CSTR):"SUB-EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-9F01-4EE7-B133-08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ][ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SAIP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-for\": \"unix:\"}"]][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-05064f74126d"][S3KY(CSTR):"SUB-EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-9F01-4EE7-B133-08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][AMID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Nachrichten zum Metadatenupdate

Audit-Meldungen werden generiert, wenn ein S3-Client die Metadaten eines Objekts aktualisiert.

Audit-Meldungen zu S3-Metadaten

Codieren	Name	Beschreibung	Verfolgen	Siehe
SUPD	S3-Metadaten wurden aktualisiert	Wird generiert, wenn ein S3-Client die Metadaten für ein aufgenommenes Objekt aktualisiert.	CBID, S3KY, HTRH	"SUPD: S3-Metadaten wurden aktualisiert"

Beispiel: S3-Metadatenaktualisierung

Das Beispiel zeigt eine erfolgreiche Transaktion zur Aktualisierung der Metadaten für ein vorhandenes S3-Objekt.

SUPD: S3-Metadatenaktualisierung

Der S3-Client fordert eine SUPD (SUPD) auf, die angegebenen Metadaten zu aktualisieren (`x-amz-meta-*`) für das S3-Objekt (S3KY). In diesem Beispiel sind Anforderungsheader im Feld HTRH enthalten, da sie als Audit-Protokoll-Header konfiguriert wurde (**KONFIGURATION > Monitoring > Audit- und Syslog-Server**). Siehe ["Konfigurieren von Überwachungsmeldungen und Protokollzielen"](#).

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\": \"identity\", \"authorization\": \"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\": \"0\", \"date\": \"Tue, 11 Jul 2017 21:54:03
GMT\", \"host\": \"10.96.99.163:18082\",
\"user-agent\": \"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\": \"/testbkt1/testobj1\", \"x-amz-metadata-
directive\": \"REPLACE\", \"x-amz-meta-city\": \"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrDplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

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.