



Format der Revisionsprotokolldatei

StorageGRID software

NetApp
July 23, 2026

Inhalt

- Format der Revisionsprotokolldatei 1
 - Erfahren Sie mehr über das Format von Revisionsprotokolldateien in StorageGRID 1
 - Verwenden Sie das Tool „audit-explain“, um StorageGRID Revisionsprotokollmeldungen zu übersetzen. . . 3
 - Verwenden Sie das Tool audit-sum, um StorageGRID-Revisionsprotokollmeldungen zusammenzufassen. 4

Format der Revisionsprotokolldatei

Erfahren Sie mehr über das Format von Revisionsprotokolldateien in StorageGRID

Die Revisionsprotokoll Logdateien befinden sich auf jedem Admin Node und enthalten eine Sammlung einzelner Audit-Meldungen.

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`

YYYY-MM-DDTHH:MM:SS.UUUUUU, wobei *UUUUUU* Mikrosekunden sind.

- Die Prüfmeldung selbst, in eckigen Klammern eingeschlossen und beginnend mit `AUDT`.

Das folgende Beispiel zeigt drei Audit-Meldungen in einer Revisionsprotokolldatei (Zeilenumbrüche wurden zur besseren Lesbarkeit hinzugefügt). Diese Meldungen wurden generiert, als ein Mandant einen S3-Bucket erstellte und diesem zwei Objekte hinzufügte.

2019-08-07T18:43:30.247711

[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142142472611085]]

2019-08-07T18:43:30.783597

[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558

[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):13489590586043706682]]

Im Standardformat sind die Audit-Meldungen in den Revisionsprotokolldateien nicht leicht lesbar oder interpretierbar. Mit ["audit-explain Tool"](#) lassen sich vereinfachte Zusammenfassungen der Audit-Meldungen im Revisionsprotokoll erhalten. Mit ["\\${post_edited_translations.segment}"](#) kann zusammengefasst werden, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge dauerten.

Verwenden Sie das Tool „audit-explain“, um StorageGRID Revisionsprotokollmeldungen zu übersetzen.

Das `audit-explain` Tool kann verwendet werden, um die Audit-Meldungen im Revisionsprotokoll in ein leicht lesbares Format zu übersetzen.

Bevor Sie beginnen

- Du hast "spezifische Zugriffsberechtigungen".
- Sie müssen über die Datei `Passwords.txt` verfügen.
- Sie müssen die IP-Adresse des primären Admin-Node kennen.

Über diese Aufgabe

Das `audit-explain` Tool, das auf dem primären Admin-Node verfügbar ist, bietet vereinfachte Zusammenfassungen der Audit-Meldungen in einem Revisionsprotokoll.



Das `audit-explain` Tool ist primär für den Einsatz durch den technischen Support bei der Fehlerbehebung vorgesehen. Die Verarbeitung von `audit-explain` Abfragen kann viel CPU-Leistung beanspruchen, was StorageGRID Vorgänge beeinträchtigen kann.

Dieses Beispiel zeigt die typische Ausgabe des `audit-explain` Tools. Diese vier "`audit-explain`" Revisionsprotokollmeldungen wurden generiert, als der S3-Tenant mit der Konto-ID 92484777680322627870 S3 PUT-Anfragen verwendete, um einen Bucket mit dem Namen „bucket1“ zu erstellen und diesem Bucket drei Objekte hinzuzufügen.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

Das `audit-explain` Tool kann Folgendes ausführen:

- Einfache oder komprimierte Revisionsprotokolle werden verarbeitet. Beispielsweise:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

- Mehrere Dateien gleichzeitig verarbeiten. Zum Beispiel:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

- Eingaben aus einer Pipe akzeptieren, was das Filtern und Vorverarbeiten der Eingabe mithilfe des `grep` Befehls oder anderer Methoden ermöglicht. Beispielsweise:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Da Revisionsprotokolle sehr groß sein und langsam analysiert werden können, lässt sich Zeit sparen, indem Sie die Teile herausfiltern, die Sie sich ansehen möchten, und `audit-explain` auf diese Teile anwenden, anstatt auf die gesamte Datei.



Das `audit-explain` Tool akzeptiert keine komprimierten Dateien als Eingabe über eine Pipe. Um komprimierte Dateien zu verarbeiten, können deren Dateinamen als Befehlszeilenargumente angegeben oder das `zcat` Tool verwendet werden, um die Dateien zuerst zu dekomprimieren. Beispielsweise:

```
zcat audit.log.gz | audit-explain
```

Die `help` (`-h`) Option zeigt die verfügbaren Optionen an. Zum Beispiel:

```
$ audit-explain -h
```

Schritte

1. `${post_edited_translations.segment}`
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
 - b. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.
 - c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
 - d. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.

Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#`.

2. Geben Sie den folgenden Befehl ein, wobei `/var/local/audit/export/audit.log` den Namen und den Speicherort der Datei oder Dateien bezeichnet, die Sie analysieren möchten:

```
$ audit-explain /var/local/audit/export/audit.log
```

Das `audit-explain` Tool gibt für Menschen lesbare Interpretationen aller Meldungen in der/den angegebenen Datei(en) aus.



Um die Zeilenlänge zu reduzieren und die Lesbarkeit zu verbessern, werden Zeitstempel standardmäßig nicht angezeigt. Wenn die Zeitstempel angezeigt werden sollen, kann die Option (`-t`) `timestamp` verwendet werden.

Verwenden Sie das Tool `audit-sum`, um StorageGRID-Revisionsprotokollmeldungen zusammenzufassen.

Das `audit-sum` Tool kann verwendet werden, um die Anzahl der Revisionsprotokoll-Meldungen für Schreiben, Lesen, Head und Löschen zu zählen sowie die minimale, maximale und durchschnittliche Zeit (oder Größe) für jeden Operationstyp anzuzeigen.

Bevor Sie beginnen

- Du hast "spezifische Zugriffsberechtigungen".
- Sie haben die `Passwords.txt` Datei.
- Sie kennen die IP-Adresse des primären Admin-Knotens.

Über diese Aufgabe

Das `audit-sum` Tool, das auf dem primären Admin-Knoten verfügbar ist, fasst zusammen, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge gedauert haben.



Das `audit-sum` Tool ist primär für den Einsatz durch den technischen Support bei der Fehlerbehebung vorgesehen. Die Verarbeitung `audit-sum` von Abfragen kann viel CPU-Leistung beanspruchen, was StorageGRID Vorgänge beeinträchtigen kann.

Dieses Beispiel zeigt die typische Ausgabe des `audit-sum` Tools. Dieses Beispiel zeigt, wie lange Protokolloperationen dauerten.

```
message group          count      min(sec)      max(sec)
average(sec)
=====
=====
IDEL                  274
SDEL                213371      0.004        20.934
0.352
SGET                201906      0.010        1740.290
1.132
SHEA                 22716      0.005         2.349
0.272
SPUT                1771398      0.011        1770.563
0.487
```

Das ``audit-sum`` Tool liefert Anzahl und Zeiten für die folgenden S3- und ILM-Audit-Meldungen in einem Revisionsprotokoll.



Prüfcodes werden aus dem Produkt und der Dokumentation entfernt, sobald Funktionen veraltet sind. Falls ein Prüfcode auftritt, der hier nicht aufgeführt ist, bieten die vorherigen Versionen dieses Themas Informationen zu älteren StorageGRID Releases. Zum Beispiel "[StorageGRID 11.8 Verwendung des audit sum Tools](#)".

Code	Beschreibung	Siehe
IDEL	ILM Initiated Delete: Protokolliert, wenn ILM den Prozess zum Löschen eines Objekts startet.	" <code>\$_{post_edited_translations.segment}</code> "
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets.	" <code>SDEL: S3-DELETE</code> "

Code	Beschreibung	Siehe
SGET	S3 GET: Protokolliert eine erfolgreiche Transaktion zum Abrufen eines Objekts oder zum Auflisten der Objekte in einem Bucket.	"SGET: S3 GET"
SHEA	S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um die Existenz eines Objekts oder Buckets zu überprüfen.	"SHEA: S3 HEAD"
<code>\${post_edited}_translations.segment}</code>	S3 PUT: Protokolliert eine erfolgreiche Transaktion zum Erstellen eines neuen Objekts oder Buckets.	"SPUT: S3 PUT"

Das `audit-sum` Tool kann Folgendes ausführen:

- Einfache oder komprimierte Revisionsprotokolle werden verarbeitet. Beispielsweise:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

- Mehrere Dateien gleichzeitig verarbeiten. Zum Beispiel:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

- Eingaben aus einer Pipe akzeptieren, was das Filtern und Vorverarbeiten der Eingabe mithilfe des `grep` Befehls oder anderer Methoden ermöglicht. Beispielsweise:

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```



Dieses Tool akzeptiert keine komprimierten Dateien als Eingabe über eine Pipe. Um komprimierte Dateien zu verarbeiten, können deren Dateinamen als Befehlszeilenargumente angegeben oder das `zcat` Tool verwendet werden, um die Dateien zuerst zu dekomprimieren. Beispiel:

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

Mithilfe von Befehlszeilenoptionen können Sie Operationen an Buckets getrennt von Operationen an Objekten zusammenfassen oder Nachrichtenübersichten nach Bucket-Name, Zeitraum oder Zieltyp gruppieren. Standardmäßig werden die minimale, maximale und durchschnittliche Operationszeit angezeigt, aber mit der `size (-s)` Option kann stattdessen die Objektgröße betrachtet werden.

Die `help (-h)` Option zeigt die verfügbaren Optionen an. Zum Beispiel:

```
$ audit-sum -h
```

Schritte

1. \${post_edited_translations.segment}

- Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
- Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.
- Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
- Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.

Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#`.

2. Wenn Sie alle Nachrichten im Zusammenhang mit Schreib-, Lese-, Head- und Löschvorgängen analysieren möchten, gehen Sie wie folgt vor:

- Geben Sie den folgenden Befehl ein, wobei `/var/local/audit/export/audit.log` den Namen und den Speicherort der Datei oder Dateien bezeichnet, die Sie analysieren möchten:

```
$ audit-sum /var/local/audit/export/audit.log
```

Dieses Beispiel zeigt die typische Ausgabe des `audit-sum` Tools. Dieses Beispiel zeigt, wie lange Protokolloperationen dauerten.

message group average (sec)	count	min (sec)	max (sec)
=====	=====	=====	=====
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

In diesem Beispiel sind SGET (S3 GET)-Operationen mit durchschnittlich 1,13 Sekunden am langsamsten, aber sowohl SGET- als auch SPUT (S3 PUT)-Operationen zeigen lange Worst-Case-Zeiten von etwa 1.770 Sekunden.

- Um die 10 langsamsten Abrufvorgänge anzuzeigen, kann der Befehl `grep` verwendet werden, um nur SGET-Nachrichten auszuwählen, und die Option `long output (-l)` kann hinzugefügt werden, um Objektpfade einzuschließen:

```
grep SGET audit.log | audit-sum -l
```

Die Ergebnisse umfassen den Typ (Objekt oder Bucket) und den Pfad, was es ermöglicht, das Revisionsprotokoll nach anderen Meldungen zu durchsuchen, die sich auf diese bestimmten Objekte

beziehen.

```
Total:          201906 operations
Slowest:        1740.290 sec
Average:         1.132 sec
Fastest:         0.010 sec
Slowest operations:
      time(usec)      source ip      type      size(B) path
      =====
1740289662  10.96.101.125      object  5663711385
backup/r9010aQ8JB-1566861764-4519.iso
1624414429  10.96.101.125      object  5375001556
backup/r9010aQ8JB-1566861764-6618.iso
1533143793  10.96.101.125      object  5183661466
backup/r9010aQ8JB-1566861764-4518.iso
      70839  10.96.101.125      object      28338
bucket3/dat.1566861764-6619
      68487  10.96.101.125      object      27890
bucket3/dat.1566861764-6615
      67798  10.96.101.125      object      27671
bucket5/dat.1566861764-6617
      67027  10.96.101.125      object      27230
bucket5/dat.1566861764-4517
      60922  10.96.101.125      object      26118
bucket3/dat.1566861764-4520
      35588  10.96.101.125      object      11311
bucket3/dat.1566861764-6616
      23897  10.96.101.125      object      10692
bucket3/dat.1566861764-4516
```

+ Anhand dieser Beispielausgabe lässt sich erkennen, dass die drei langsamsten S3 GET-Anfragen Objekte mit einer Größe von jeweils etwa 5 GB betrafen, die deutlich größer sind als die übrigen Objekte. Die große Größe erklärt die langen Abrufzeiten im ungünstigsten Fall.

3. Wenn Sie ermitteln möchten, welche Größen von Objekten in Ihr Grid eingelesen und daraus abgerufen werden, verwenden Sie die Option Größe (-s):

```
audit-sum -s audit.log
```

message group average (MB)	count	min (MB)	max (MB)
=====	=====	=====	=====
IDEL 1654.502	274	0.004	5000.000
SDEL 1.695	213371	0.000	10.504
SGET 14.920	201906	0.000	5000.000
SHEA 2.967	22716	0.001	10.504
SPUT 2.495	1771398	0.000	5000.000

In diesem Beispiel liegt die durchschnittliche Objektgröße für SPUT unter 2,5 MB, aber die durchschnittliche Größe für SGET ist deutlich größer. Die Anzahl der SPUT-Nachrichten ist wesentlich höher als die Anzahl der SGET-Nachrichten, was darauf hindeutet, dass die meisten Objekte nie abgerufen werden.

4. Wenn festgestellt werden soll, ob die Abrufe gestern langsam waren:

- a. Den Befehl im entsprechenden Revisionsprotokoll mit der Option group-by-time (-gt) ausführen, gefolgt vom Zeitraum (z. B. 15M, 1H, 10S):

```
grep SGET audit.log | audit-sum -gt 1H
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
2019-09-05T00 1.254	7591	0.010	1481.867
2019-09-05T01 1.115	4173	0.011	1740.290
2019-09-05T02 1.562	20142	0.011	1274.961
2019-09-05T03 1.254	57591	0.010	1383.867
2019-09-05T04 1.405	124171	0.013	1740.290
2019-09-05T05 1.562	420182	0.021	1274.511
2019-09-05T06 5.562	1220371	0.015	6274.961
2019-09-05T07 2.002	527142	0.011	1974.228
2019-09-05T08 1.105	384173	0.012	1740.290
2019-09-05T09 1.354	27591	0.010	1481.867

Diese Ergebnisse zeigen, dass der S3 GET-Traffic zwischen 06:00 und 07:00 sprunghaft anstieg. Sowohl die maximale als auch die durchschnittliche Zeit waren in diesem Zeitraum deutlich höher und stiegen nicht allmählich mit zunehmender Anzahl an. Diese Kennzahlen deuten darauf hin, dass die Kapazität überschritten wurde, möglicherweise im Netzwerk oder in der Fähigkeit des Grids, Anfragen zu verarbeiten.

- b. Um zu ermitteln, welche Größe die gestern stündlich abgerufenen Objekte hatten, die Option (-s) zum Befehl hinzufügen:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

message group average(B)	count	min(B)	max(B)
=====	=====	=====	=====
2019-09-05T00 1.976	7591	0.040	1481.867
2019-09-05T01 2.062	4173	0.043	1740.290
2019-09-05T02 2.303	20142	0.083	1274.961
2019-09-05T03 1.182	57591	0.912	1383.867
2019-09-05T04 1.528	124171	0.730	1740.290
2019-09-05T05 2.398	420182	0.875	4274.511
2019-09-05T06 51.328	1220371	0.691	5663711385.961
2019-09-05T07 2.147	527142	0.130	1974.228
2019-09-05T08 1.878	384173	0.625	1740.290
2019-09-05T09 1.354	27591	0.689	1481.867

Diese Ergebnisse deuten darauf hin, dass einige sehr große Abrufe stattfanden, als das gesamte Abrufaufkommen seinen Höhepunkt erreichte.

- c. Um weitere Details anzuzeigen, kann die Funktion ["audit-explain Tool"](#) verwendet werden, um alle SGET Operationen während dieser Stunde zu überprüfen:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Falls die Ausgabe des grep-Befehls voraussichtlich aus vielen Zeilen besteht, kann der less Befehl hinzugefügt werden, um den Inhalt der Revisionsprotokoll-Datei seitenweise (bildschirmweise) anzuzeigen.

5. Wenn Sie feststellen möchten, ob SPUT-Operationen auf Buckets langsamer sind als SPUT-Operationen auf Objekten:

- a. Beginnen Sie mit der Option `-go`, die Meldungen für Objekt- und Bucket-Operationen separat gruppiert:

```
grep SPUT sample.log | audit-sum -go
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.bucket 0.125	1	0.125	0.125
SPUT.object 0.236	12	0.025	1.019

Die Ergebnisse zeigen, dass SPUT-Operationen für Buckets andere Leistungsmerkmale aufweisen als SPUT-Operationen für Objekte.

- b. Um festzustellen, welche Buckets die langsamsten SPUT-Operationen aufweisen, kann die `-gb` Option verwendet werden, die Nachrichten nach Bucket gruppiert:

```
grep SPUT audit.log | audit-sum -gb
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.cho-non-versioning 1.571	71943	0.046	1770.563
SPUT.cho-versioning 1.415	54277	0.047	1736.633
SPUT.cho-west-region 1.329	80615	0.040	55.557
SPUT.ldt002 0.361	1564563	0.011	51.569

- c. Um zu ermitteln, welche Buckets die größte SPUT-Objektgröße aufweisen, sollten sowohl die `-gb` als auch die `-s` Optionen verwendet werden:

```
grep SPUT audit.log | audit-sum -gb -s
```

message group average(B)	count	min(B)	max(B)
=====	=====	=====	=====
=====			
SPUT.cho-non-versioning 21.672	71943	2.097	5000.000
SPUT.cho-versioning 21.120	54277	2.097	5000.000
SPUT.cho-west-region 14.433	80615	2.097	800.000
SPUT.ldt002 0.352	1564563	0.000	999.972

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.