



# Format der Auditprotokolldatei

## StorageGRID

NetApp  
March 12, 2025

# Inhalt

- Format der Auditprotokolldatei ..... 1
- Format der Auditprotokolldatei ..... 1
- Verwenden Sie das Audit-Erklären-Tool ..... 3
- Verwenden Sie das Audit-Sum-Tool ..... 4

# Format der Auditprotokolldatei

## Format der Auditprotokolldatei

Die Audit-Log-Dateien befinden sich auf jedem Admin-Knoten und enthalten eine Sammlung einzelner Audit-Nachrichten.

Jede Überwachungsmeldung enthält Folgendes:

- Die koordinierte Weltzeit (UTC) des Ereignisses, das die Meldung (ATIM) im ISO 8601-Format auslöste, gefolgt von einem Leerzeichen:

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

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

Das folgende Beispiel zeigt drei Audit-Nachrichten in einer Audit-Log-Datei (Zeilenumbrüche zur Lesbarkeit hinzugefügt). Diese Meldungen wurden generiert, wenn ein Mandant einen S3-Bucket erstellt und diesem Bucket zwei Objekte hinzugefügt hat.

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]]
```

In ihrem Standardformat sind die Überwachungsmeldungen in den Audit-Log-Dateien nicht einfach zu lesen oder zu interpretieren. Mit dem können Sie vereinfachte Zusammenfassungen der ["Audit-Explain-Tool"](#) Überwachungsmeldungen im Überwachungsprotokoll abrufen. Mithilfe des können Sie ["Audit-Summe-Tool"](#) zusammenfassen, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge gedauert haben.

# Verwenden Sie das Audit-Erklären-Tool

Sie können das Tool verwenden `audit-explain`, um die Audit-Meldungen im Audit-Protokoll in ein leicht lesbares Format zu übersetzen.

## Bevor Sie beginnen

- Sie haben "Bestimmte Zugriffsberechtigungen".
- Sie müssen über die `Passwords.txt` Datei verfügen.
- Sie müssen die IP-Adresse des primären Admin-Knotens kennen.

## Über diese Aufgabe

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



Das `audit-explain` Tool ist in erster Linie für den Einsatz durch den technischen Support bei der Fehlerbehebung vorgesehen. Verarbeitungsabfragen `audit-explain` können eine hohe CPU-Leistung verbrauchen, was sich auf die StorageGRID-Vorgänge auswirken kann.

Dieses Beispiel zeigt eine typische Ausgabe des `audit-explain` Tools. Diese vier "SPUT" Audit-Meldungen wurden generiert, als der S3-Mandant mit Konto-ID 92484777680322627870 S3-PUT-Anfragen verwendete, um einen Bucket mit dem Namen „bucket1“ zu erstellen und drei Objekte zu diesem Bucket 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 tun:

- Verarbeiten Sie einfache oder komprimierte Prüfprotokolle. Beispiel:

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

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

- Mehrere Dateien gleichzeitig verarbeiten. Beispiel:

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

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

- Eingaben von einer Pipe akzeptieren, wodurch Sie die Eingabe mit dem Befehl oder anderen Mitteln filtern und vorverarbeiten `grep` können. Beispiel:

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

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

Da Audit-Protokolle sehr groß und langsam zu analysieren sind, können Sie Zeit sparen, indem Sie Teile filtern, die Sie auf den Teilen betrachten und ausführen möchten `audit-explain`, anstatt der gesamten Datei.



Das `audit-explain` Tool akzeptiert keine komprimierten Dateien als Piped-Eingabe. Um komprimierte Dateien zu verarbeiten, geben Sie ihre Dateinamen als Befehlszeilenargumente ein, oder verwenden Sie das `zcat` Tool, um die Dateien zuerst zu dekomprimieren. Beispiel:

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

Verwenden Sie die `help` (`-h`) Option, um die verfügbaren Optionen anzuzeigen. Beispiel:

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

### Schritte

1. Melden Sie sich beim primären Admin-Node an:
  - a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
  - b. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.
  - c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
  - d. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

Wenn Sie als root angemeldet sind, wechselt die Eingabeaufforderung von `$` zu `#`.

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

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

Das `audit-explain` Tool druckt menschenlesbare Interpretationen aller Meldungen in der angegebenen Datei oder Datei.



Um die Linienlänge zu verringern und die Lesbarkeit zu erleichtern, werden Zeitstempel standardmäßig nicht angezeigt. Wenn Sie die Zeitstempel sehen möchten, verwenden Sie die (`-t`Option timestamp`).

## Verwenden Sie das Audit-Sum-Tool

Mit dem Tool können `audit-sum` Sie die Audit-Meldungen schreiben, lesen, Kopf und löschen sowie die minimale, maximale und durchschnittliche Zeit (oder Größe) für jeden Operationsart anzeigen.

### Bevor Sie beginnen

- Sie haben "[Bestimmte Zugriffsberechtigungen](#)".
- Sie müssen über die `Passwords.txt` Datei verfügen.

- Sie müssen die IP-Adresse des primären Admin-Knotens kennen.

### Über diese Aufgabe

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



Das `audit-sum` Tool ist in erster Linie für den Einsatz durch den technischen Support bei der Fehlerbehebung vorgesehen. Verarbeitungsabfragen `audit-sum` können eine hohe CPU-Leistung verbrauchen, was sich auf die StorageGRID-Vorgänge auswirken kann.

Dieses Beispiel zeigt eine typische Ausgabe des `audit-sum` Tools. Dieses Beispiel zeigt, wie lange Protokollvorgänge dauerte.

```

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 bietet Zählungen und Uhrzeiten für die folgenden S3-, Swift- und ILM-Audit-Meldungen in einem Revisionsprotokoll.



Audit-Codes werden aus dem Produkt und der Dokumentation entfernt, da Funktionen veraltet sind. Wenn ein Audit-Code angezeigt wird, der hier nicht aufgeführt ist, überprüfen Sie die früheren Versionen dieses Themas auf ältere SG-Versionen. "[StorageGRID 11.8 mit der Dokumentation des Audit Sum Tools](#)"Beispiel: .

| Codieren | Beschreibung   | Siehe   |
|----------|--|---|
| IDEL     | ILM initiated Delete: Protokolliert, wenn ILM den Prozess des Löschens eines Objekts startet.                              | " <a href="#">IDEL: ILM gestartet Löschen</a> " |
| SDEL     | S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets.                             | " <a href="#">SDEL: S3 LÖSCHEN</a> "            |
| SGET     | S3 GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Bucket aufzulisten. | " <a href="#">SGET S3 ABRUFEN</a> "             |

| Codieren | Beschreibung   | Siehe                       |
|----------|--|-----------------------------|
| SHEA     | S3 HEAD: Protokolliert eine erfolgreiche Transaktion, um zu überprüfen, ob ein Objekt oder ein Bucket vorhanden ist.             | "SHEA: S3 KOPF"             |
| SPUT     | S3 PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Bucket zu erstellen.                   | "SPUT: S3 PUT"              |
| WDEL     | Swift DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Containers.                             | "WDEL: Swift LÖSCHEN"       |
| WGET     | Swift GET: Protokolliert eine erfolgreiche Transaktion, um ein Objekt abzurufen oder die Objekte in einem Container aufzulisten. | "WGET: Schneller ERHALTEN"  |
| WHEA     | Swift HEAD: Protokolliert eine erfolgreiche Transaktion, um das Vorhandensein eines Objekts oder Containers zu überprüfen.       | "WHEA: Schneller KOPF"      |
| WPUT     | Swift PUT: Protokolliert eine erfolgreiche Transaktion, um ein neues Objekt oder einen neuen Container zu erstellen.             | "WPUT: Schnell AUSGEDRÜCKT" |

Das `audit-sum` Tool kann Folgendes tun:

- Verarbeiten Sie einfache oder komprimierte Prüfprotokolle. Beispiel:

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

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

- Mehrere Dateien gleichzeitig verarbeiten. Beispiel:

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

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

- Eingaben von einer Pipe akzeptieren, wodurch Sie die Eingabe mit dem Befehl oder anderen Mitteln filtern und vorverarbeiten `grep` können. Beispiel:

```
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 Piper Input. Um komprimierte Dateien zu verarbeiten, geben Sie ihre Dateinamen als Befehlszeilenargumente ein, oder verwenden Sie das `zcat` Tool, um die Dateien zuerst zu dekomprimieren. Beispiel:

```
audit-sum audit.log.gz

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

Mit Befehlszeilenoptionen können Operationen für Buckets separat von Operationen für Objekte zusammengefasst oder Nachrichtenübersichten nach Bucket-Namen, Zeitraum oder Zieltyp gruppieren. Standardmäßig werden in den Zusammenfassungen die minimale, maximale und durchschnittliche Betriebsdauer angezeigt, Sie können jedoch die Option verwenden, um die `size` (-s) Objektgröße zu überprüfen.

Verwenden Sie die `help` (-h) Option, um die verfügbaren Optionen anzuzeigen. Beispiel:

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

### Schritte

1. Melden Sie sich beim primären Admin-Node an:

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

Wenn Sie als root angemeldet sind, wechselt die Eingabeaufforderung von \$ zu #.

2. Wenn Sie alle Nachrichten analysieren möchten, die mit Schreibvorgängen, Lese-, Kopf- und Löschvorgängen zusammenhängen, führen Sie die folgenden Schritte aus:

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

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

Dieses Beispiel zeigt eine typische Ausgabe des `audit-sum` Tools. Dieses Beispiel zeigt, wie lange Protokollvorgänge dauerte.

| message group<br>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) Vorgänge im Durchschnitt mit 1.13 Sekunden die langsamsten. SGET und SPUT (S3 PUT) Vorgänge weisen jedoch lange Schlimmstfallszeiten von etwa 1,770 Sekunden auf.

- b. Um die langsamsten 10 Abruffunktionen anzuzeigen, verwenden Sie den grep-Befehl, um nur SGET-Nachrichten auszuwählen und die Long-Ausgabeoption hinzuzufügen(-l, um Objektpfade einzuschließen):

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

Die Ergebnisse umfassen den Typ (Objekt oder Bucket) und den Pfad, mit dem Sie das Audit-Protokoll für andere Meldungen zu diesen speziellen Objekten grep erstellen können.

```

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

```

+ Aus diesem Beispielausgang sehen Sie, dass die drei langsamsten S3-GET-Anfragen für Objekte mit einer Größe von ca. 5 GB waren, was viel größer ist als die anderen Objekte. Die große Größe berücksichtigt die langsamen Abrufzeiten im schlimmsten Fall.

3. Wenn Sie festlegen möchten, welche Größe von Objekten in Ihr Raster aufgenommen und aus diesem abgerufen werden soll, verwenden Sie die Größenoption (-s):

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

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

In diesem Beispiel liegt die durchschnittliche Objektgröße für SPUT unter 2.5 MB, die durchschnittliche Größe für SGET ist jedoch deutlich größer. Die Anzahl der SPUT-Meldungen ist viel höher als die Anzahl der SGET-Nachrichten, was darauf hinweist, dass die meisten Objekte nie abgerufen werden.

4. Wenn Sie feststellen möchten, ob die Abrufvorgänge gestern langsam waren:
  - a. Geben Sie den Befehl im entsprechenden Audit-Protokoll ein und verwenden Sie die Option Group-by-time (-gt), gefolgt von dem Zeitraum (z.B. 15M, 1H, 10S):

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

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

Diese Ergebnisse zeigen, dass S3 VERKEHR zwischen 06:00 und 07:00 Spikes. Auch die max- und Durchschnittszeiten sind zu diesen Zeiten deutlich höher, und sie stiegen nicht schrittweise auf, wenn die Zahl erhöht wurde. Dies deutet darauf hin, dass die Kapazität irgendwo überschritten wurde, vielleicht im Netzwerk oder in der Fähigkeit des Grids, Anfragen zu verarbeiten.

- b. Um zu bestimmen, welche Größe Objekte wurden abgerufen jede Stunde gestern, fügen Sie die Größe Option (-s), um den Befehl:

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

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

Diese Ergebnisse zeigen, dass einige sehr große Rückrufe auftraten, als der gesamte Abrufverkehr seinen maximalen Wert hatte.

c. Weitere Informationen finden Sie im, "[Audit-Explain-Tool](#)" um alle SGET-Vorgänge während der betreffenden Stunde zu überprüfen:

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

Wenn die Ausgabe des grep-Befehls viele Zeilen enthalten soll, fügen Sie den Befehl hinzu, um den less Inhalt der Audit-Log-Datei jeweils eine Seite (ein Bildschirm) anzuzeigen.

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

a. Mit der Option wird gestartet `-go`, bei der Meldungen für Objekt- und Bucket-Vorgänge getrennt gruppiert werden:

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

| message group | count | min(sec) | max(sec) |
|---------------|-------|----------|----------|
| SPUT.bucket   | 1     | 0.125    | 0.125    |
| SPUT.object   | 12    | 0.025    | 1.019    |

Die Ergebnisse zeigen, dass SPUT-Operationen für Buckets unterschiedliche Leistungseigenschaften haben als SPUT-Operationen für Objekte.

b. Um zu ermitteln, welche Buckets die langsamsten SPUT-Vorgänge haben, verwenden Sie die `-gb` Option, welche Meldungen nach Bucket gruppiert:

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

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

c. Um zu ermitteln, welche Buckets die größte SPUT-Objektgröße aufweisen, verwenden Sie die `-gb` Optionen und `-s`:

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

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



## Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtlich geschützten Urhebers 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.