Audit-Protokolldateiformat

StorageGRID software

NetApp
October 21, 2025

Inhalt

Audit-Protokolldateiformat

Audit-Protokolldateiformat

Die Audit-Protokolldateien befinden sich auf jedem Admin-Knoten und enthalten eine Sammlung einzelner Audit-Meldungen.

Jede Prüfnachricht enthält Folgendes:

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

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

- Die Prüfnachricht selbst, eingeschlossen in eckige Klammern und beginnend mit `AUDT` .

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

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][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(F
C32):S3RQ][ATID(UI64):84396067221084560 22]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][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(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

In ihrem Standardformat sind die Prüfmeldungen in den Prüfprotokolldateien nicht einfach zu lesen oder zu interpretieren. Sie können die"Audit-Erklärtool" um vereinfachte Zusammenfassungen der Audit-Meldungen im Audit-Protokoll zu erhalten. Sie können die"Auditsummen-Tool" um zusammenzufassen, wie viele Schreib-, Lese- und Löschvorgänge protokolliert wurden und wie lange diese Vorgänge dauerten.

Verwenden Sie das Audit-Explain-Tool

Sie können die `audit-explain` Tool zum Übersetzen der Audit-Meldungen im Audit-

Protokoll in ein leicht lesbares Format.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Der `audit-explain` Das auf dem primären Admin-Knoten verfügbare Tool bietet vereinfachte Zusammenfassungen der Audit-Meldungen in einem Audit-Protokoll.

> Der `audit-explain` Das Tool ist in erster Linie für die Verwendung durch den technischen Support bei der Fehlerbehebung vorgesehen. Verarbeitung `audit-explain` Abfragen können eine große Menge an CPU-Leistung verbrauchen, was sich auf den Betrieb von StorageGRID auswirken kann.

Dieses Beispiel zeigt eine typische Ausgabe des `audit-explain` Werkzeug. Diese vier"SPUT" Es wurden Prüfmeldungen generiert, als der S3-Mandant 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
```

Der `audit-explain` Das Tool kann Folgendes:

- Verarbeiten Sie einfache oder komprimierte Prüfprotokolle. Beispiel:

  ```
  audit-explain audit.log

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

- Verarbeiten Sie mehrere Dateien gleichzeitig. Beispiel:

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

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

- Akzeptieren Sie Eingaben von einer Pipe, die es Ihnen ermöglicht, die Eingabe mithilfe der `grep` Befehl oder andere Mittel. Beispiel:

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

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

Da Audit-Protokolle sehr groß und langsam zu analysieren sein können, können Sie Zeit sparen, indem Sie Teile filtern, die Sie ansehen möchten, und ausführen `audit-explain` auf die Teile, statt auf die gesamte Datei.

> Der `audit-explain` Das Tool akzeptiert keine komprimierten Dateien als Pipe-Eingabe. Um komprimierte Dateien zu verarbeiten, geben Sie deren Dateinamen als Befehlszeilenargumente an oder verwenden Sie die `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-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

      Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .
2. Geben Sie den folgenden Befehl ein, wobei `/var/local/log/audit.log` stellt den Namen und den Speicherort der Datei(en) dar, die Sie analysieren möchten:

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

   Der `audit-explain` Das Tool druckt für Menschen lesbare Interpretationen aller Nachrichten in der bzw. den angegebenen Dateien.

   > Um die Zeilenlänge zu reduzieren und die Lesbarkeit zu verbessern, werden Zeitstempel standardmäßig nicht angezeigt. Wenn Sie die Zeitstempel sehen möchten, verwenden Sie den Zeitstempel(`-t`) Option.

Verwenden Sie das Audit-Sum-Tool

Sie können die `audit-sum` Tool zum Zählen der Prüfnachrichten zum Schreiben, Lesen, Kopfzeilen und Löschen und zum Anzeigen der minimalen, maximalen und durchschnittlichen Zeit (oder Größe) für jeden Vorgangstyp.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

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

> Der `audit-sum` Das Tool ist in erster Linie für die Verwendung durch den technischen Support bei der Fehlerbehebung vorgesehen. Verarbeitung `audit-sum` Abfragen können eine große Menge an CPU-Leistung verbrauchen, was sich auf den Betrieb von StorageGRID auswirken kann.

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

Der `audit-sum` Das Tool stellt Anzahl und Zeit für die folgenden S3-, Swift- und ILM-Auditmeldungen in einem Audit-Protokoll bereit.

> Prüfcodes werden aus dem Produkt und der Dokumentation entfernt, wenn Funktionen veraltet sind. Wenn Sie auf einen Prüfcode stoßen, der hier nicht aufgeführt ist, überprüfen Sie die vorherigen Versionen dieses Themas auf ältere SG-Versionen. Beispiel: "StorageGRID 11.8 Dokumentation zum Verwenden des Auditsummentools" .

Code	Beschreibung	Siehe
IDEL	Von ILM initiiertes Löschen: Protokolliert, wenn ILM den Löschvorgang eines Objekts startet.	"IDEL: Von ILM initiiertes Löschen"
SDEL	S3 DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Buckets.	"SDEL: S3 LÖSCHEN"
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 KOPF"

Code	Beschreibung	Siehe
SPUT	S3 PUT: Protokolliert eine erfolgreiche Transaktion zum Erstellen eines neuen Objekts oder Buckets.	"SPUT: S3 PUT"
WDEL	Swift DELETE: Protokolliert eine erfolgreiche Transaktion zum Löschen eines Objekts oder Containers.	"WDEL: Schnelles LÖSCHEN"
WGET	Swift GET: Protokolliert eine erfolgreiche Transaktion zum Abrufen eines Objekts oder zum Auflisten der Objekte in einem Container.	"WGET: Schnelles GET"
WHEA	Swift HEAD: Protokolliert eine erfolgreiche Transaktion, um die Existenz eines Objekts oder Containers zu überprüfen.	"WHEA: Schneller Kopf"
WPUT	Swift PUT: Protokolliert eine erfolgreiche Transaktion zum Erstellen eines neuen Objekts oder Containers.	"WPUT: Schnelles PUT"

Der `audit-sum` Das Tool kann Folgendes:

- Verarbeiten Sie einfache oder komprimierte Prüfprotokolle. Beispiel:

```
audit-sum audit.log

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

- Verarbeiten Sie mehrere Dateien gleichzeitig. Beispiel:

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

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

- Akzeptieren Sie Eingaben von einer Pipe, die es Ihnen ermöglicht, die Eingabe mithilfe der `grep` Befehl oder andere Mittel. 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 Pipe-Eingabe. Um komprimierte Dateien zu verarbeiten, geben Sie deren Dateinamen als Befehlszeilenargumente an oder verwenden Sie die `zcat` Tool, um die Dateien zuerst zu dekomprimieren. Beispiel:
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

Sie können Befehlszeilenoptionen verwenden, um Vorgänge für Buckets getrennt von Vorgängen für Objekte

zusammenzufassen oder um Meldungszusammenfassungen nach Bucket-Name, Zeitraum oder Zieltyp zu gruppieren. Standardmäßig zeigen die Zusammenfassungen die minimale, maximale und durchschnittliche Betriebszeit an, Sie können jedoch die `size (-s)` Option, stattdessen die Objektgröße zu betrachten.

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

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

Schritte

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

      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, führen Sie die folgenden Schritte aus:
   a. Geben Sie den folgenden Befehl ein, wobei `/var/local/log/audit.log` stellt den Namen und den Speicherort der Datei(en) dar, die Sie analysieren möchten:

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

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

      In diesem Beispiel sind SGET-Operationen (S3 GET) mit durchschnittlich 1,13 Sekunden am langsamsten, aber SGET- und SPUT-Operationen (S3 PUT) weisen beide lange Worst-Case-Zeiten von etwa 1.770 Sekunden auf.

   b. Um die 10 langsamsten Abrufvorgänge anzuzeigen, verwenden Sie den Befehl grep, um nur SGET-Nachrichten auszuwählen und die Option für die lange Ausgabe hinzuzufügen(`-l`), um Objektpfade

einzuschließen:

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

Die Ergebnisse umfassen den Typ (Objekt oder Bucket) und den Pfad, sodass Sie das Prüfprotokoll nach anderen Nachrichten durchsuchen können, 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/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-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 können Sie erkennen, dass die drei langsamsten S3-GET-Anfragen für Objekte mit einer Größe von etwa 5 GB waren, was viel größer ist als die anderen Objekte. Die große Größe ist für die langsamen Abrufzeiten im schlimmsten Fall verantwortlich.

3. Wenn Sie bestimmen möchten, welche Objektgrößen in Ihr Raster aufgenommen und daraus abgerufen werden, verwenden Sie die Größenoption(`-s`):

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

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

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

4. Wenn Sie feststellen möchten, ob die Abrufe gestern langsam waren:

   a. Führen Sie den Befehl für das entsprechende Überwachungsprotokoll aus und verwenden Sie die Option „Nach Zeit gruppieren“.(`-gt`), gefolgt vom Zeitraum (z. B. 15M, 1H, 10S):

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

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

Diese Ergebnisse zeigen, dass der S3 GET-Verkehr zwischen 06:00 und 07:00 Uhr seinen Höhepunkt erreichte. Auch die Höchst- und Durchschnittszeiten sind zu diesen Zeiten erheblich höher und steigen nicht allmählich an, wenn die Anzahl steigt. Dies deutet darauf hin, dass irgendwo die Kapazität überschritten wurde, vielleicht im Netzwerk oder bei der Fähigkeit des Grids, Anfragen zu verarbeiten.

b. Um zu ermitteln, welche Objektgröße gestern stündlich abgerufen wurde, fügen Sie die Option „Größe“ hinzu(`-s`) zum Befehl:

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

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

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

c. Um weitere Details anzuzeigen, verwenden Sie die"Audit-Erklärtool" um alle SGET-Operationen während dieser Stunde zu überprüfen:

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

Wenn die Ausgabe des grep-Befehls voraussichtlich viele Zeilen umfasst, fügen Sie die `less` Befehl, um den Inhalt der Prüfprotokolldatei seitenweise (bildschirmweise) anzuzeigen.

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

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

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

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

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

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

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

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

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

```
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

Markeninformationen