审核日志文件格式

StorageGRID

NetApp
October 03, 2025

目录

审核日志文件格式

审核日志文件位于每个管理节点上，其中包含一组单独的审核消息。

每个审核消息都包含以下内容：

- 触发审核消息（ ATIM ）的事件的协调世界时（ UTC ），格式为 ISO 8601 ，后跟一个空格：

  `YYYY-MM-DDTHH： MM： SS.UUUUUUU_`，其中 `*UUUU*` 为微秒。

- 审核消息本身，括在方括号内，以 `AUDT` 开头。

以下示例显示了一个审核日志文件中的三条审核消息（为便于阅读，添加了换行符）。这些消息是在租户创建 S3 存储分段并向该存储分段添加两个对象时生成的。

```
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::17530064241597054
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::17530064241597054
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):8439606722108456022]]

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::17530064241597054
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]]
```

以默认格式，审核日志文件中的审核消息不易阅读或解释。您可以使用 `audit-explain` 工具获取审核日志中审核消息的简化摘要。您可以使用 `audit-sum` 工具总结已记录的写入，读取和删除操作的数量以及这些操作所需的时间。

相关信息

使用审核解释工具

使用 audit-sum 工具

使用审核解释工具

您可以使用 `audit-explain` 工具将审核日志中的审核消息转换为易于阅读的格式。

您需要的内容

- 您必须具有特定的访问权限。
- 您必须具有 `passwords.txt` 文件。
- 您必须知道主管理节点的 IP 地址。

关于此任务

主管理节点上提供的 `audit-explain` 工具可在审核日志中简化审核消息的摘要。

> `audit-explain` 工具主要供技术支持在故障排除操作期间使用。处理 **审核 - 解释** 查询可能会占用大量 CPU 资源，这可能会影响 StorageGRID 操作。

此示例显示了 `audit-explain` 工具的典型输出。当帐户 ID 为 92484777680322627870 的 S3 租户使用 S3 PUT 请求创建名为 "Bucket1" 的存储分段并向该存储分段添加三个对象时，会生成这四条 SPUT 审核消息。

```
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
```

`audit-explain` 工具可以处理简单或压缩的审核日志。例如：

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

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

`audit-explain` 工具还可以同时处理多个文件。例如：

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

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

最后， `audit-explain` 工具可以接受来自管道的输入，这样，您可以使用 `grep` 命令或其他方法筛选和预处理输入。例如：

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

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

由于审核日志可能非常大且解析速度较慢，因此您可以通过筛选要查看的部分并在这些部分（而不是整个文件）上运行 `audit-explain` 来节省时间。

`audit-explain` 工具不接受将压缩文件作为管道输入。要处理压缩的文件，请将其文件名作为命令行参数提供，或者使用 `zcat` 工具先解压缩这些文件。例如：

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

使用 `help` （ `-h` ） 选项查看可用选项。例如：

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

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
2. 输入以下命令，其中 ` /var/local/audit/export/audit.log` 表示要分析的一个或多个文件的名称和位置：

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

   `audit-explain` 工具可为指定文件中的所有消息输出可供用户读取的解释。

   为了缩短行长度并提高可读性，默认情况下不会显示时间戳。如果要查看时间戳，请使用 timestamp （` -t` ）选项。

相关信息

SPUT： S3 PUT

使用 audit-sum 工具

您可以使用 `audit-sum` 工具对写入，读取，标头和删除审核消息进行计数，并查看每种操作类型的最小，最大和平均时间（或大小）。

您需要的内容

- 您必须具有特定的访问权限。

- 您必须具有 `passwords.txt` 文件。
- 您必须知道主管理节点的 IP 地址。

关于此任务

主管理节点上提供的 `audit-sum` 工具总结了记录的写入，读取和删除操作数量以及这些操作所需的时间。

> `audit-sum` 工具主要供技术支持在故障排除操作期间使用。处理 `audit-sum` 查询可能会占用大量 CPU 资源，这可能会影响 StorageGRID 操作。

此示例显示了 `audit-sum` 工具的典型输出。此示例显示了协议操作所需的时间。

```
  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
```

`audit-sum` 工具可在审核日志中提供以下 S3 ， Swift 和 ILM 审核消息的计数和时间：

代码	**Description**	请参见
ARCT	从云层检索归档	ARCT ： 从云层检索归档
上一个月	归档存储云层	SCT ： 归档存储云层
标识	ILM Initiated Delete ： 记录 ILM 开始删除对象的过程。	idel ： ILM 已启动删除
SDEL	S3 delete ： 记录成功的事务以删除对象或存储分段。	SDEL ： S3 delete
SGET	S3 GET ： 记录成功的事务以检索对象或列出存储分段中的对象。	SGET ： S3 GET
Shea	S3 head ： 记录成功的事务以检查是否存在对象或存储分段。	Shea ： S3 机头

代码	**Description**	请参见
SPUT	S3 PUT ： 记录成功的事务以创建新对象或存储分段。	SPUT ： S3 PUT
WDEL	Swift delete ： 记录成功的事务以删除对象或容器。	WDEL ： Swift delete
wget	Swift get ： 记录成功的事务以检索对象或列出容器中的对象。	WGET ： Swift GET
WHEA	Swift head ： 记录成功的事务以检查是否存在对象或容器。	WHEA ： Swift head
WWPUT	Swift PUT ： 记录成功的事务以创建新对象或容器。	WWPUT ： Swift PUT

`audit-sum` 工具可以处理纯审核日志或压缩的审核日志。例如：

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

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

`audit-sum` 工具还可以同时处理多个文件。例如：

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

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

最后， `audit-sum` 工具还可以接受来自管道的输入，这样，您可以使用 `grep` 命令或其他方法筛选和预处理输入。例如：

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

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

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

此工具不接受将压缩文件作为管道输入。要处理压缩的文件，请将其文件名作为命令行参数提供，或者使用 `zcat` 工具先解压缩这些文件。例如：

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

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

您可以使用命令行选项将存储分段上的操作与对象上的操作分开进行汇总，或者按存储分段名称，时间段或目标类型对消息摘要进行分组。默认情况下，摘要会显示最小，最大和平均操作时间，但您可以使用 `size` （ `-s` ） 选项查看对象大小。

使用 `help` （ `-h` ） 选项查看可用选项。例如：

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

步骤

1. 登录到主管理节点：
   a. 输入以下命令： `ssh admin@ primary_Admin_Node_IP_`
   b. 输入 `passwords.txt` 文件中列出的密码。
2. 如果要分析与写入，读取，磁头和删除操作相关的所有消息，请执行以下步骤：
   a. 输入以下命令，其中 ` /var/local/audit/export/audit.log` 表示要分析的一个或多个文件的名称和位置：

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

      此示例显示了 `audit-sum` 工具的典型输出。此示例显示了协议操作所需的时间。

      ```
        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
      ```

在此示例中， SGET （ S3 GET ）操作的平均速度最慢，为 1.13 秒，但 SGET 和 SPUT （ S3 PUT ）操作的最坏情况时间都较长，约为 1 ， 770 秒。

b. 要显示速度最慢的 10 个检索操作，请使用 grep 命令仅选择 SGET 消息，并添加较长的输出选项（` -l` ）以包含对象路径： `grep SGET audit.log ； audit-sum -l`

结果包括类型（对象或分段）和路径，您可以通过此类结果在审核日志中添加与这些特定对象相关的其他消息。

```
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
```

+ 在此示例输出中，您可以看到，三个最慢的 S3 GET 请求针对的是大小约为 5 GB 的对象，该大小远远大于其他对象。大容量导致最差情况检索时间较慢。

3. 如果要确定要将哪些大小的对象输入网格并从网格中检索到，请使用 size 选项（` -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
```

在此示例中， SPUT 的平均对象大小小于 2.5 MB ，但 SGET 的平均大小要大得多。SPUT 消息的数量远远高于 SGET 消息的数量，这表明大多数对象永远不会被检索到。

4. 如果要确定昨天的检索速度是否较慢：

   a. 在相应的审核日志上输入命令并使用 group-by-time 选项（` -gt` ），后跟时间段（例如 15M ， 1H ， 10S ）问题描述：

      ```
      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
```

这些结果显示 S3 GET 流量在 06： 00 到 07： 00 之间达到高峰。这些时间的最大和平均时间也明显较高，并且不会随着数量的增加而逐渐增加。这表明容量已超出某个位置，可能是在网络中，也可能是在网格处理请求的能力中。

b. 要确定昨天每小时检索的对象大小，请在命令中添加 size 选项（` -s` ）：

```
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
```

这些结果表明，当整体检索流量达到最大值时，会发生一些非常大的检索。

c. 要查看更多详细信息，请使用 `audit-explain` 工具查看该时段的所有 SGET 操作：

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

如果 grep 命令的输出应为多行，请添加 `less` 命令，以便一次显示一页（一个屏幕）的审核日志文件内容。

5. 如果要确定存储分段上的 SPUT 操作是否比对象的 SPUT 操作慢：

a. 首先使用 ` -go` 选项，该选项可分别对对象和存储分段操作的消息进行分组：

```
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
```

结果显示，存储分段的 SPUT 操作与对象的 SPUT 操作具有不同的性能特征。

b. 要确定哪些存储分段的 SPUT 操作最慢，请使用 ` -GB` 选项，该选项可按存储分段对消息进行分组：

```
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. 要确定哪些分段的 SPUT 对象大小最大，请使用 ` -GB` 和 ` -s` 选项：

```
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
```

相关信息

使用审核解释工具

版权信息

商标信息