



审核日志文件格式 StorageGRID software

NetApp
July 23, 2026

目录

- 审核日志文件格式..... 1
 - 了解 StorageGRID 中审计日志文件的格式 1
 - 使用 audit-explain 工具翻译 StorageGRID 审核消息..... 2
 - 使用 audit-sum 工具汇总 StorageGRID 审核消息 4

审核日志文件格式

了解 **StorageGRID** 中审计日志文件的格式

审核日志文件位于每个管理节点上，包含各个审核消息的集合。

每条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)，采用 ISO 8601 格式，后跟空格：

`YYYY-MM-DDTHH:MM:SS.UUUUUU`，其中 `'UUUUUU'` 为微秒。

- 审核消息本身，括在方括号内并以 `'AUDT'` 开头。

以下示例显示了审计日志文件中的三条审计消息（为可读性添加了换行符）。当租户创建 S3 存储桶并将两个对象添加到该存储桶时，会生成这些消息。

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):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::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]]
```

在默认格式中，审核日志文件中的审核消息不容易阅读或解释。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"](#) 汇总记录了多少次写入、读取和删除操作以及这些操作花费了多长时间。

使用 **audit-explain** 工具翻译 **StorageGRID** 审核消息

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。

开始之前

- 您有 "特定访问权限"。
- 您必须具有该 `Passwords.txt` 文件。
- `\${post\_edited\_translations.segment}`

关于此任务

该 `audit-explain` 工具位于主管理节点上，可在审计日志中提供审计消息的简化摘要。



该 audit-explain 工具主要供技术支持人员在故障排除操作期间使用。处理 audit-explain 查询可能会消耗大量的 CPU 资源，从而可能影响 StorageGRID 的运行。

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" 的存储桶并向该存储桶添加三个对象时，会生成这四个 "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
```

该 `audit-explain` 工具可以执行以下操作：

- 处理纯文本或压缩的审计日志。例如：

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

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

- 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/*
```

- 接受来自管道的输入，这允许您使用 grep 命令或以其他方式对输入进行过滤和预处理。例如：

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

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

由于审计日志可能非常大且解析速度较慢，您可以通过过滤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。



该 `audit-explain` 工具不接受压缩文件作为管道输入。要处理压缩文件，请提供其文件名作为命令行参数，或先使用 `zcat` 工具解压缩文件。例如：

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

使用 `help (-h)` 选项可查看可用选项。例如：

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

步骤

1. \${post_edited_translations.segment}

- 输入以下命令： `ssh admin@primary_Admin_Node_IP`
- 输入 `Passwords.txt` 文件中列出的密码。
- 输入以下命令切换到 root： `su -`
- 输入 `Passwords.txt` 文件中列出的密码。

以 root 身份登录时，提示符将从 `$` 更改为 `#`。

2. 输入以下命令，其中 `/var/local/audit/export/audit.log` 表示您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
```

该 `audit-explain` 工具打印指定一个或多个文件中所有消息的人类可读解释。



为了减少行长并提高可读性，默认情况下不显示时间戳。如果要查看时间戳，请使用 `timestamp (-t)` 选项。

使用 **audit-sum** 工具汇总 **StorageGRID** 审核消息

您可以使用该 `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短、最大和平均时间（或大小）。

开始之前

- 您有 "特定访问权限"。
- 您拥有 `Passwords.txt` 文件。
- 您知道主管理节点的 IP 地址。

关于此任务

该 `audit-sum` 工具可在主管理节点上使用，它汇总了记录的写入、读取和删除操作的数量以及这些操作所用的时间。



该 `audit-sum` 工具主要供技术支持人员在故障排除操作期间使用。处理 `audit-sum` 查询可能会消耗大量 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花费的时间。

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			

该 `audit-sum` 工具在审核日志中提供以下 S3 和 ILM 审核消息的计数和时间。



审核代码将随功能弃用而从产品和文档中删除。如果遇到此处未列出的审核代码，请查看本主题的早期版本以了解较旧的 StorageGRID 版本。例如，"[\\${post_edited_translations.segment}](#)"。

代码	问题描述	请参阅
IDEL	ILM Initiated Delete：在 ILM 开始删除对象的过程时记录日志。	" IDEL：ILM Initiated Delete "
SDEL	S3 DELETE：记录成功删除对象或存储桶的事务。	" SDEL：S3 DELETE "
SGET	S3 GET：记录成功的事务以检索对象或列出存储桶中的对象。	" SGET：S3 GET "
SHEA	S3 HEAD：记录成功的事务以检查对象或存储桶是否存在。	" SHEA：S3 HEAD "
SPUT	S3 PUT：记录成功的事务以创建新对象或存储桶。	" SPUT：S3 PUT "

该 `audit-sum` 工具可以执行以下操作：

- 处理纯文本或压缩的审计日志。例如：

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

- 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/*
```

- 接受来自管道的输入，这允许您使用 `grep` 命令或以其他方式对输入进行过滤和预处理。例如：

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

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

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



此工具不接受压缩文件作为管道输入。要处理压缩文件，请提供其文件名作为命令行参数，或者先使用 `zcat` 工具解压缩文件。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区上的操作与对象上的操作分开汇总，或按存储区名称、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)'` 选项可查看可用选项。例如：

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

步骤

1. `${post_edited_translations.segment}`

- 输入以下命令：`ssh admin@primary_Admin_Node_IP`
- 输入 `'Passwords.txt'` 文件中列出的密码。
- 输入以下命令切换到 `root`：`su -`
- 输入 `'Passwords.txt'` 文件中列出的密码。

以 `root` 身份登录时，提示符将从 `$` 更改为 ``#`。

2. 如果要分析与写入、读取、HEAD和DELETE操作相关的所有消息，请执行以下步骤：

- 输入以下命令，其中 `/var/local/audit/export/audit.log` 表示您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花费的时间。

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			

在此示例中，SGET（S3 GET）操作平均最慢，为 1.13 秒，但 SGET 和 SPUT（S3 PUT）操作都显示了约 1,770 秒的最坏情况时间。

b. 要显示最慢的 10 个检索操作，请使用 `grep` 命令仅选择 SGET 消息并添加 `long` 输出选项(-l) 以包含对象路径：

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

`${post_edited_translations.segment}`

```

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

```

+ 从此示例输出中，您可以看到三个最慢的 S3 GET 请求是针对大小约为 5 GB 的对象，比其他对象大得多。较大的大小导致最坏情况下的检索时间较慢。

3. 如果要确定从网格中摄取和检索的对象的大小，请使用大小选项(-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

在此示例中，SPUT 的平均对象大小低于 2.5 MB，但 SGET 的平均大小要大得多。SPUT 消息的数量远高于 SGET 消息的数量，这表明大多数对象从未被检索过。

4. 如果要确定昨天的检索速度是否很慢：

- a. 在相应的审核日志上运行该命令，并使用按时间分组选项 (-gt)，后跟时间段（例如 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

这些结果表明，S3 GET 流量在 06:00 到 07:00 之间出现激增。在此时间段内，最大时间和平均时间均明显更高，并且它们并没有随着次数的增加而逐渐递增。这些指标表明容量已超出，可能是网络容量超限，也可能是网络处理请求的能力超限。

b. 要确定昨天每小时检索了哪些大小的对象，请向命令中添加大小选项 (-s)：

```
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

这些结果表明，当总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"](#) 查看该小时内的所有 SGET 操作：

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

如果 `grep` 命令的输出预计为多行，请添加 ``less`` 命令，以每次一页（一个屏幕）的方式显示审核日志文件的内容。

5. 如果要确定存储桶上的 SPUT 操作是否比对象的 SPUT 操作慢：

a. 首先使用 `-go` 选项，该选项将对象和存储桶操作的消息分别进行分组：

```
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

`${post_edited_translations.segment}`

- b. 要确定哪些存储桶的 SPUT 操作最慢，请使用 `-gb`` 选项，该选项按存储桶对消息进行分组：

```
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. 要确定哪些存储桶的 SPUT 对象大小最大，请同时使用 `-gb` 和 `-s` 选项：

```
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

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。