查看审核日志

StorageGRID software

NetApp
July 23, 2026

目录

查看审核日志 . . . 1
审核消息和日志 . . . 1
审核消息如何通过 StorageGRID 系统移动到 audit.log 文件以进行保留 . . . 1
审核消息流 . . . 1
从 StorageGRID 管理节点命令行访问审核日志文件 . . . 4
了解 StorageGRID 中的审核日志文件轮换 . . . 5
审核日志文件格式 . . . 5
了解 StorageGRID 中审计日志文件的格式 . . . 5
使用 audit-explain 工具翻译 StorageGRID 审核消息 . . . 6
使用 audit-sum 工具汇总 StorageGRID 审核消息 . . . 8
审核消息格式 . . . 17
了解 StorageGRID 审核消息的结构 . . . 17
StorageGRID 审核消息中的数据类型 . . . 18
StorageGRID 审核消息中的事件特定数据 . . . 18
StorageGRID 审核消息中的常见元素 . . . 19
StorageGRID 审核消息格式和示例 . . . 20
审核消息和对象生命周期 . . . 21
在 StorageGRID 中生成审核消息时 . . . 21
StorageGRID 中对象摄取事务的审核消息 . . . 22
StorageGRID 中对象删除事务的审核消息 . . . 24
StorageGRID 中对象检索事务的审核消息 . . . 25
StorageGRID 中 S3 对象元数据更新的审核消息 . . . 27
审核消息 . . . 28
了解 StorageGRID 中的审计消息类型和代码 . . . 28
审核消息类别 . . . 28
审核消息参考 . . . 32

查看审核日志

审核消息和日志

这些说明包含有关 StorageGRID 审计消息和审计日志的结构和内容的信息。您可以使用此信息阅读和分析系统活动的审计跟踪。

这些说明适用于负责生成系统活动和使用情况报告的管理员，这些报告需要分析 StorageGRID 系统的审计消息。

要使用文本日志文件，必须能够访问管理节点上配置的审计共享。

有关配置审核消息级别和使用外部 syslog 服务器的信息，请参见 "配置日志管理和外部 syslog 服务器"。

审核消息如何通过 StorageGRID 系统移动到 audit.log 文件以进行保留

所有 StorageGRID 服务在正常系统操作期间生成审核消息。您应该了解这些审核消息如何通过 StorageGRID 系统移动到 `audit.log`文件。

以下审核消息和审核消息保留的工作流程仅适用于为 **Admin Nodes/local nodes** 或 **Admin Node and external syslog server** 配置的 StorageGRID。如果 StorageGRID 配置为"Local nodes only"（默认）或"External syslog server"，则审核消息将本地保存在每个节点的 `/var/local/log/localaudit.log`文件中，且无法由 Admin Nodes 或 Storage Nodes 处理。

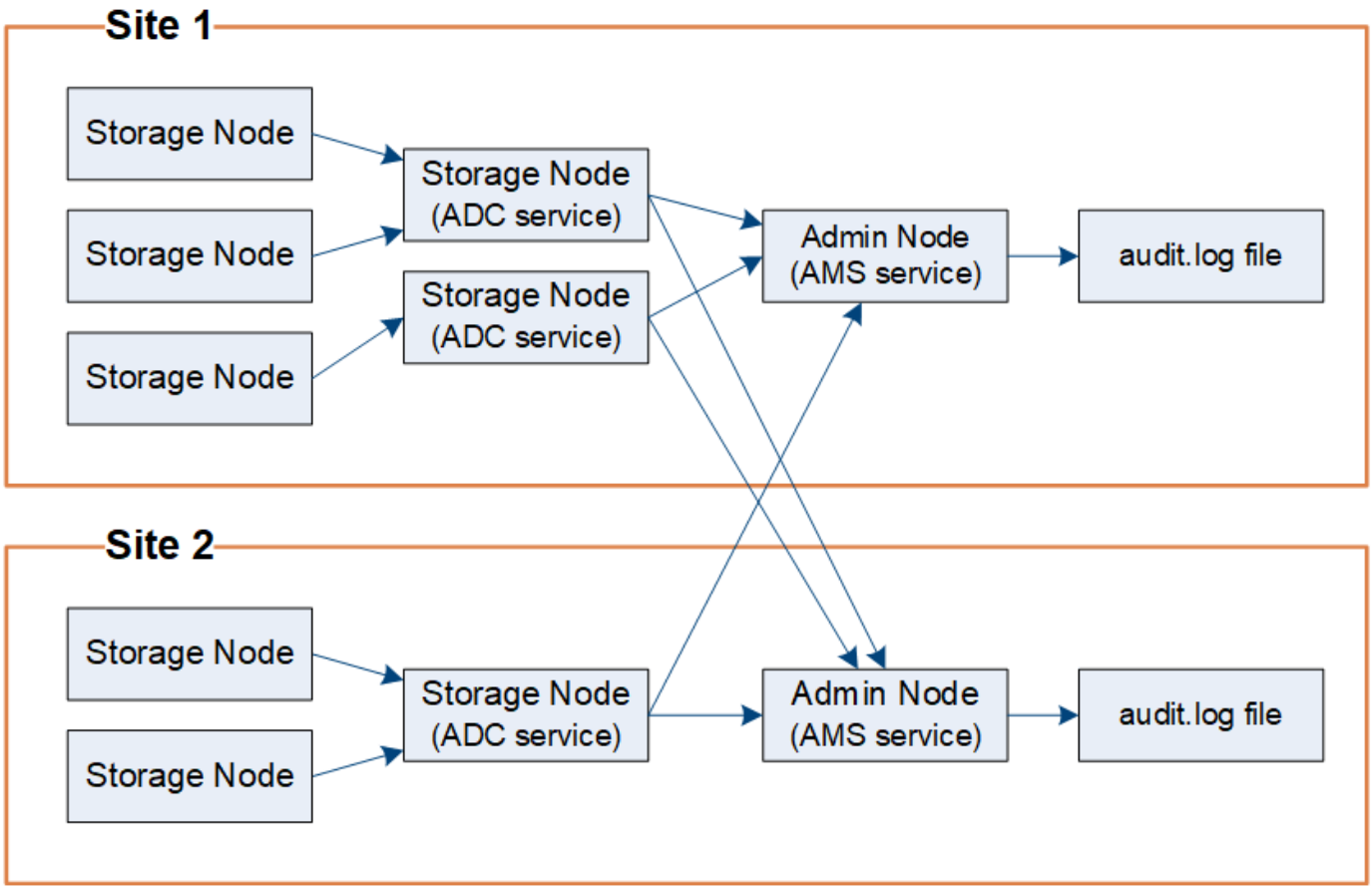
审核消息流

当 StorageGRID 配置为*管理节点/本地节点*或*管理节点和外部 syslog 服务器*时，审核消息由管理节点以及具有管理域控制器 (ADC) 服务的存储节点处理。

如审核消息流程图所示，每个 StorageGRID 节点都会将其审核消息发送到数据中心站点的 ADC 服务之一。ADC 服务将自动为每个站点上安装的前三个存储节点启用。

反过来，每个ADC服务都充当中继，并将其审计消息集合发送到StorageGRID系统中的每个管理节点，从而为每个管理节点提供系统活动的完整记录。

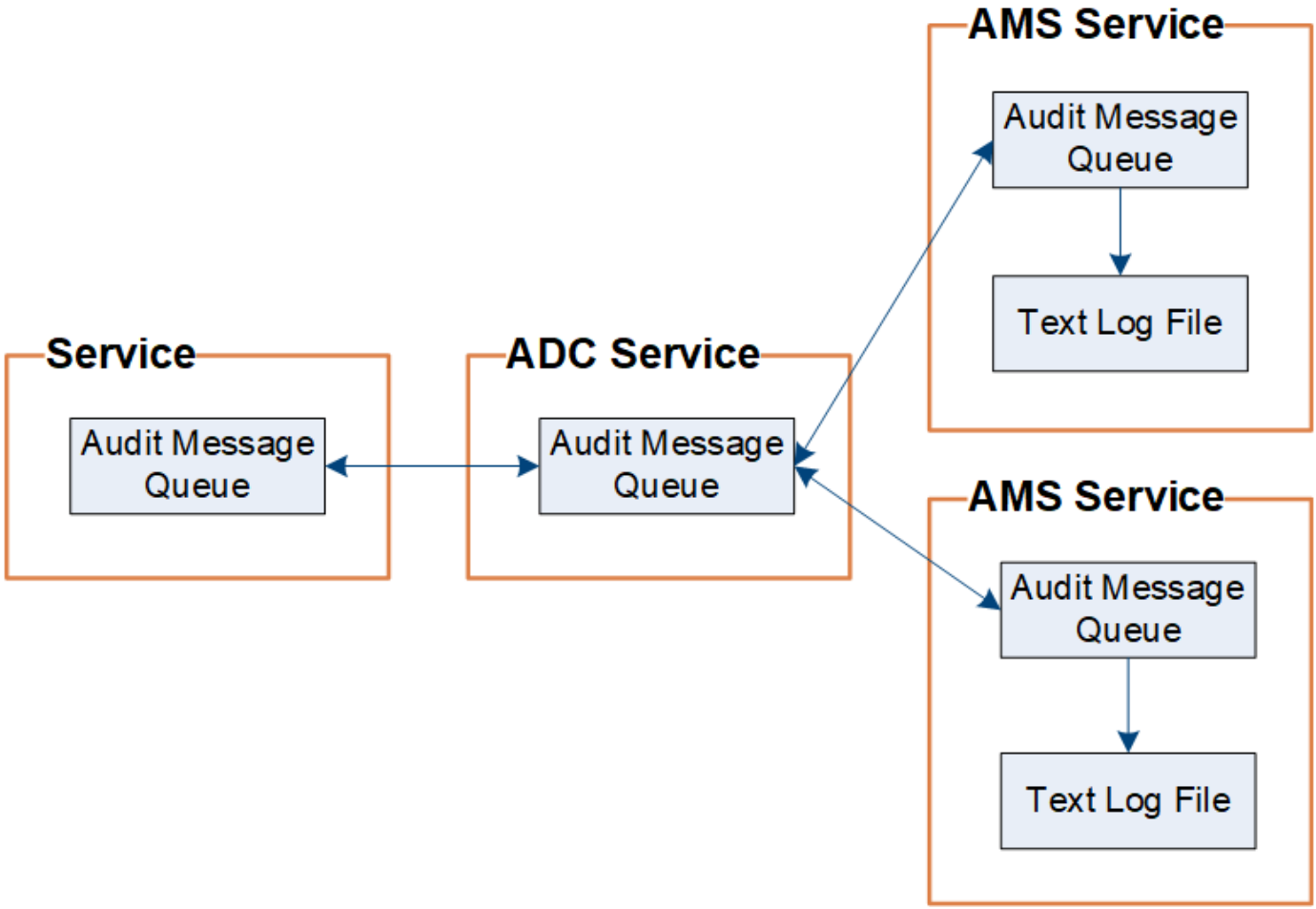
每个管理节点将审核消息存储在文本日志文件中；活动日志文件名为 `audit.log`。



审核消息保留

StorageGRID 使用复制和删除流程，以确保审核消息在写入审核日志之前不会丢失。

当节点生成或中继审核消息时，该消息存储在网格节点系统磁盘上的审核消息队列中。消息的副本始终保存在审核消息队列中，直到消息被写入管理节点 `/var/local/audit/export`目录中的审核日志文件。这有助于防止在传输过程中丢失审核消息。



由于网络连接问题或审核容量不足，审核消息队列可能会暂时增加。随着队列的增加，它们会占用每个节点的`/var/local/`目录中更多的可用空间。如果问题仍然存在，且节点的审核消息目录已过满，则各个节点将优先处理其积压工作，并暂时无法接收新消息。

具体而言，您可能会看到以下行为：

- 如果管理节点使用 `/var/local/audit/export`的目录已满，则管理节点将被标记为不可用于新审核消息，直到目录不再满为止。S3 客户端请求不受影响。当审核存储库无法访问时，会触发 XAMS（无法访问的审核存储库）警报。
- 如果具有 ADC 服务的存储节点使用的 `/var/local/`目录已满 92%，则该节点将被标记为不可用于审核消息，直到目录仅满 87%。S3 客户端对其他节点的请求不受影响。当无法访问审核中继时，会触发 NRLY（可用审核中继）警报。

> 如果没有带有 ADC 服务的可用存储节点，则存储节点将审计消息本地存储在`/var/local/log/localaudit.log`文件中。

- 如果 Storage Node 使用的 `/var/local/`目录已满 85%，则该节点将开始拒绝 S3 客户端请求，并返回 `503 Service Unavailable`。

以下类型的问题可能导致审核消息队列增长非常大：

- 使用 ADC 服务的管理节点或存储节点的中断。如果系统的某个节点出现故障，则其余节点可能会出现积压。

- ${post_edited_translations.segment}
- ADC 存储节点上的 `/var/local/` 空间因与审计消息无关的原因而变满。发生这种情况时，该节点将停止接受新的审计消息，并优先处理其当前的积压工作，这可能会导致其他节点上出现积压。

${post_edited_translations.segment}

为了帮助您随时间监控审核消息队列的大小，当存储节点队列或管理节点队列中的消息数量达到特定阈值时，会触发 **Large audit queue** 警报和旧版 AMQS 警报。

${post_edited_translations.segment}

如果警报或警示持续存在且严重程度增加，请查看队列大小图表。如果该数值在数小时或数天内持续增加，则审计负载可能已超过系统的审计容量。通过将“Client Writes”（客户端写入）和“Client Reads”（客户端读取）的审计级别更改为“Error”（错误）或“Off”（关闭），可以降低客户端操作速率或减少记录的审计消息数量。请参见 "配置日志管理和外部 syslog 服务器"。

重复消息

如果发生网络或节点故障，StorageGRID 系统会采取保守的方法。因此，审核日志中可能会存在重复的消息。

从 StorageGRID 管理节点命令行访问审核日志文件

审核共享包含活动 `audit.log`文件和任何压缩的审核日志文件。您可以直接从管理节点的命令行访问审核日志文件。

除非您为 管理节点/本地节点 或 管理节点和外部 **syslog** 服务器 配置 StorageGRID，否则 `audit.log`文件将保持为空。有关详细信息，请参阅 "选择日志位置"。

开始之前

- 您有 "特定访问权限"。
- 您必须具有该 `Passwords.txt`文件。
- 您必须知道管理节点的 IP 地址。

步骤

1. 登录到管理节点：
   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。
   c. 输入以下命令切换到 root： `su -`
   d. 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. ${post_edited_translations.segment}

   ```
   cd /var/local/audit/export/
   ```
3. ${post_edited_translations.segment}

了解 StorageGRID 中的审核日志文件轮换

如果 StorageGRID 配置为 **Admin Nodes/local nodes** 或 **Admin Node and external syslog server**，则审核日志文件将保存到 Admin Node 的 `/var/local/audit/export/`目录中。活动审核日志文件命名为 `audit.log`。

> 也可以更改审核日志的目标，并将审核信息发送到外部 syslog 服务器。配置外部 syslog 服务器时，将继续生成和存储审核记录的本地日志。请参阅 "配置审核消息和外部 syslog 服务器"。

每天一次，活动 `audit.log`文件将被保存，并启动一个新的 `audit.log`文件。已保存文件的名称以格式 `*yyyy-mm-dd.txt*`表示其保存时间。如果在一天内创建了多个审核日志，文件名将使用文件保存的日期，并附加一个数字，格式为 `*yyyy-mm-dd.txt.n*`。例如，`2018-04-15.txt`和 `2018-04-15.txt.1`是2018年4月15日创建和保存的第一个和第二个日志文件。

一天后，保存的文件将被压缩并重命名，格式为 *yyyy-mm-dd.txt.gz*，该格式保留原始日期。随着时间的推移，分配给审核日志的管理节点存储将被消耗。脚本监控审核日志空间消耗，并根据需要删除日志文件，以释放 `/var/local/audit/export/`目录中的空间。审核日志将根据其创建日期进行删除。最旧的日志将首先删除。您可以在以下文件中监视脚本的操作： `/var/local/log/manage-audit.log`。

此示例显示活动 `audit.log`文件、前一天的文件（`2018-04-15.txt`）和前一天的压缩文件(`2018-04-14.txt.gz`）。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

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::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]]
```

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}
   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。
   c. 输入以下命令切换到 root： `su -`
   d. 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           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
```

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}
   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。
   c. 输入以下命令切换到 root： `su -`
   d. 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：
   a. 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           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/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
```

+ 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            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           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，也可能是网格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           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           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
```

${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                  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                    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
```

审核消息格式

了解 StorageGRID 审核消息的结构

在 StorageGRID 系统内交换的审核消息包括所有消息通用的标准信息以及描述所报告事件或活动的特定内容。

如果"audit-explain"和"audit-sum"工具提供的摘要信息不足，请参阅本节以了解所有审计消息的一般格式。

下面是审核日志文件中可能出现的审核消息示例：

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

每个审核消息都包含一个属性元素字符串。整个字符串用括号括起来(`[ ]`），字符串中的每个属性元素具有以下特点：

- 括在括号中 `[ ]`
- 由字符串 `AUDT`引入，表示审核消息
- 前后不带分隔符（无逗号或空格）
- 由换行符终止 `\n`

每个元素都包含以下格式报告的属性代码、数据类型和值：

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

消息中的属性元素数量取决于消息的事件类型。属性元素不按任何特定顺序列出。

以下列表描述了属性元素：

- `ATTR` 是所报告属性的四个字符的代码。有些属性是所有审计消息共有的，有些属性则是特定于事件的。
- `type` 是值编程数据类型的四个字符的标识符，例如 UI64、FC32 等。该类型用括号括起来 `( )`。
- `value` 是属性的内容，通常是数值或文本值。值始终跟在冒号 (`:` 后面）。数据类型为 CSTR 的值用双引号 " " 括起来。

StorageGRID 审核消息中的数据类型

不同的数据类型用于在审核消息中存储信息。

类型	问题描述
UI32	无符号长整数（32位）；它可以存储数字 0 到 4,294,967,295。
UI64	无符号双长整数（64 位）；它可以存储 0 到 18,446,744,073,709,551,615 的数字。
FC32	四字符常量；32 位无符号整数值，表示为四个 ASCII 字符，例如"ABCD"。
IPAD	用于 IP 地址。
CSTR	可变长度的 UTF-8 字符数组。字符可以使用以下约定进行转义： • 反斜杠为\\。 • 回车符为 \r。 • 双引号为\"。 • 换行符（新行）为 \n。 • 字符可以替换为其十六进制等效字符（格式为 \xHH，其中 HH 是表示该字符的十六进制值）。

StorageGRID 审核消息中的事件特定数据

审核日志中的每个审核消息都记录特定于系统事件的数据。

在用于标识消息本身的起始 `[AUDT:`容器之后，下一组属性将提供有关审计消息所描述的事件或操作的信息。以下示例中突出显示了这些属性：

```
2018-12-05T08:24:45.921845 [AUDT: \[RSLT\(FC32\):SUCS\]
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025
621595611246499"\]
\[SACC\(CSTR\):"account"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dY
zKlumRsKJA=="\]
\[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"account"\]\[S3BK\(C
STR\):"bucket"\]
\[S3KY\(CSTR\):"object"\]\[CBID\(UI64\):0xCC128B9B9E428347\]
\[UUID\(CSTR\):"B975D2CE-E4DA-4D14-8A23-
1CB4B83F2CD8"\]\[CSIZ\(UI64\):30720\][AVER(UI32):10]
\[ATIM(UI64):1543998285921845]\[ATYP\(FC32\):SHEA\][ANID(UI32):12281045][A
MID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261]]
```

The `ATYP` 元素（在示例中带下划线）标识生成消息的事件。此示例消息包括"SHEA"消息代码（[ATYP(FC32):SHEA]），表示它是由成功的 S3 HEAD 请求生成的。

StorageGRID 审核消息中的常见元素

所有审核消息都包含通用元素。

代码	类型	问题描述
AMID	FC32	模块 ID：生成消息的模块 ID 的四字符标识符。这表示生成审核消息的代码段。
ANID	UI32	节点 ID：分配给生成消息的服务的网格节点 ID。在配置和安装 StorageGRID 系统时，每个服务都会分配一个唯一标识符。此 ID 无法更改。
ASES	UI64	审核会话标识符：在以前的版本中，此元素指示服务启动后审核系统初始化的时间。此时间值以微秒为单位，自操作系统纪元（1970 年 1 月 1 日 00:00:00 UTC）起计算。 注： 此元素已过时，不再显示在审核消息中。
ASQN	UI64	序列计数：在以前的版本中，对于网格节点 (ANID) 上生成的每个审核消息，此计数器都会递增，并在服务重新启动时重置为零。 注： 此元素已过时，不再显示在审核消息中。
ATID	UI64	跟踪 ID：由单个事件触发的一组消息共享的标识符。

代码	类型	问题描述
ATIM	UI64	时间戳：触发审核消息的事件生成时间，以操作系统时期（1970 年 1 月 1 日 00:00:00 UTC）以来的微秒为单位。请注意，将时间戳转换为本地日期和时间的大多数可用工具基于毫秒。 可能需要对记录的时间戳进行四舍五入或截断。 `audit.log`文件中审核消息开头显示的人工可读时间是 `ISO 8601` 格式的 `ATIM` 属性。日期和时间表示为 `*YYYY-MMDDTHH:MM:SS.UUUUUU*`，其中 `T`是表示日期时间段开头的文字字符串字符。`*UUUUUU*`为微秒。
ATYP	FC32	事件类型：正在记录的事件的四字符标识符。这决定了消息的"有效负载"内容：包含的属性。
平均	UI32	版本：审核消息的版本。随着 StorageGRID 软件的发展，新版本的服务可能会在审计报告中加入新功能。此字段可在 AMS 服务中实现向后兼容性，以处理来自旧版本服务的消息。
RSLT	FC32	结果：事件、流程或事务的结果。如果与消息无关，则使用 NONE 而非 SUCS，以免意外过滤消息。

StorageGRID 审核消息格式和示例

您可以在每条审核消息中找到详细信息。所有审核消息都使用相同的格式。

以下是审计消息示例，该消息可能出现在 `audit.log`文件中：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

审核消息包含有关正在记录的事件的信息，以及有关审核消息本身的信息。

要识别审核消息记录的是哪个事件，请查找 ATYP 属性（下面突出显示）：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

ATYP 属性的值为 SPUT。"SPUT" 表示 S3 PUT 事务，该事务将对象的摄取记录到存储桶。

以下审核消息还显示了与对象关联的存储区：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

要发现 PUT 事件何时发生，请注意审核消息开头的通用协调时间 (UTC) 时间戳。此值是审核消息本身的 ATIM 属性的人类可读版本：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM记录自UNIX纪元开始以来的时间，以微秒为单位。在该示例中，该值 `1405631878959669`转换为2014年7月17日星期四 21:17:59 UTC。

审核消息和对象生命周期

在 StorageGRID 中生成审核消息时

每次摄入、检索或删除对象时，都会生成审计消息。您可以通过定位特定于 S3 API 的审计消息，在审计日志中识别这些交易。

${post_edited_translations.segment}

协议	代码
链接 S3 操作	S3BK（存储桶）、S3KY（密钥）或两者
链接内部操作	CBID（对象的内部标识符）

审核消息的时间安排

由于网格节点之间的时间差异、对象大小和网络延迟等因素，不同服务生成的审核消息的顺序可能与本节示例中所示的顺序不同。

StorageGRID 中对象摄取事务的审核消息

您可以通过查找 S3 API 特定的审核消息，在审核日志中识别客户端摄取事务。

并非在接收事务期间生成的所有审核消息都列在下表中。仅包括跟踪接收事务所需的消息。

S3 提取审核消息

代码	名称	问题描述	跟踪	请参见
SPUT	S3 PUT 事务	S3 PUT 摄取事务已成功完成。	CBID、S3BK、S3KY	"SPUT：S3 PUT"
ORLM	满足对象规则	已满足此对象的 ILM 策略。	CBID	"ORLM：Object Rules Met"

示例：**S3** 对象提取

以下一系列审核消息是当 S3 客户端将对象摄入到存储节点（LDR 服务）时生成并保存到审核日志中的审核消息的示例。

在此示例中，活动 ILM 策略包括 Make 2 Copies ILM 规则。

> 并非事务期间生成的所有审计消息都列在下面的示例中。仅列出与 S3 摄取事务 (SPUT) 相关的内容。

此示例假定先前已创建 S3 存储桶。

SPUT：S3 PUT

生成 SPUT 消息以指示已发出 S3 PUT 事务以在特定存储桶中创建对象。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM：Object Rules Met

ORLM 消息指示此对象已满足 ILM 策略。消息包括对象的 CBID 和应用的 ILM 规则的名称。

对于复制的对象，LOCS 字段包括对象位置的 LDR 节点 ID 和卷 ID。

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

对于纠删码对象，LOCS 字段包括纠删码配置文件 ID 和纠删码组 ID

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

路径字段包括 S3 存储桶和密钥信息。

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

StorageGRID 中对象删除事务的审核消息

您可以通过查找 S3 API 特定的审核消息，在审核日志中识别对象删除事务。

下表中未列出删除事务期间生成的所有审核消息。仅包括跟踪删除事务所需的消息。

S3 删除审核消息

代码	名称	问题描述	跟踪	请参见
SDEL	S3 删除	请求从存储桶中删除对象。	CBID, S3KY	"SDEL：S3 DELETE"

示例：**S3** 对象删除

当 S3 客户端从存储节点（LDR 服务）中删除对象时，会生成审核消息并保存到审核日志中。

> 并非删除事务期间生成的所有审核消息都列在下面的示例中。仅列出与 S3 删除事务 (SDEL) 相关的内容。

SDEL：S3 Delete

当客户端向 LDR 服务发送 DeleteObject 请求时，对象删除开始。消息包含要从中删除对象的存储桶和对象的 S3 Key，用于标识对象。

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

StorageGRID 中对象检索事务的审核消息

您可以通过查找 S3 API 特定的审核消息，在审核日志中识别对象检索事务。

并非在检索事务期间生成的所有审核消息都会在下表中列出。仅包括跟踪检索事务所需的消息。

S3检索审核消息

代码	名称	问题描述	跟踪	请参见
SGET	S3 GET	从存储桶检索对象的请求。	CBID、S3BK、S3KY	"SGET：S3 GET"

示例：**S3** 对象检索

当 S3 客户端从存储节点（LDR 服务）检索对象时，会生成审核消息并保存到审核日志中。

请注意，并非所有在事务期间生成的审核消息都列在下面的示例中。仅列出与 S3 检索事务 (SGET) 相关的内容。

SGET：S3 GET

当客户端向 LDR 服务发送 GetObject 请求时，对象检索开始。消息包含从中检索对象的存储桶和对象的 S3 Key，用于标识对象。

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

如果存储桶策略允许，客户端可以匿名检索对象，或者可以从不同租户帐户拥有的存储桶中检索对象。审核消息包含有关存储桶所有者租户帐户的信息，以便可以跟踪这些匿名和跨帐户请求。

在以下示例消息中，客户端发送 GetObject 请求，以获取存储在其不拥有的存储桶中的对象。SBAI 和 SBAC 的值记录存储桶所有者的租户帐户 ID 和名称，这与 S3AI 和 SACC 中记录的客户端租户帐户 ID 和名称不同。

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

示例：**S3 Select** 对象

当 S3 客户端在对象上发出 S3 Select 查询时，将生成审核消息并保存到审核日志中。

请注意，并非所有在事务期间生成的审核消息都列在下面的示例中。仅列出与 S3 Select 事务（SelectObjectContent）相关的内容。

每个查询会生成两条审核消息：一条用于执行 S3 Select 请求的授权（S3SR 字段设置为 "select"），另一条是在处理过程中从存储中检索数据的后续标准 GET 操作。

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

StorageGRID 中 S3 对象元数据更新的审核消息

当 S3 客户端更新对象的元数据时，系统会生成审核消息。

S3元数据更新审核消息

代码	名称	问题描述	跟踪	请参见
SUPD	S3 元数据已更新	当 S3 客户端更新已摄取对象的元数据时生成。	CBID、S3KY、HTRH	"SUPD：S3 元数据已更新"

示例：**S3** 元数据更新

此示例显示用于更新现有 S3 对象的元数据的成功事务。

SUPD: S3元数据更新

S3 客户端发出请求 (SUPD)，以更新 S3 对象 (S3KY) 的指定元数据(`x-amz-meta-*`。在此示例中，请求标头包含在 HTRH 字段中，因为它已配置为审核协议标头（*Configuration* > **Monitoring** > **Audit and syslog server**）。请参阅"配置日志管理和外部 syslog 服务器"。

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

审核消息

了解 StorageGRID 中的审计消息类型和代码

以下各节列出了系统返回的审计消息的详细说明。每个审计消息首先在表格中列出，该表格按消息表示的活动类别对相关消息进行分组。这些分组对于了解被审计的活动类型以及选择所需的审计消息过滤类型都很有用。

审核消息还按其四个字符代码的字母顺序列出。通过此字母列表，您可以查找有关特定消息的信息。

本章中使用的四个字符代码是审计消息中找到的 ATYP 值，如下面的示例消息所示：

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

有关设置审核消息级别、更改日志目标以及使用外部 syslog 服务器获取审核信息的信息，请参见 "配置日志管理和外部 syslog 服务器"

审核消息类别

属于系统审核类别的审核消息用于与审核系统本身、网格节点状态、全系统任务活动（网格任务）和服务备份操作相关的事件。

代码	消息标题和描述	请参见
ECMC	缺少擦除编码数据片段：表示检测到缺少擦除编码数据片段。	"ECMC：缺少擦除编码数据片段"
ECOC	损坏的擦除编码数据片段：表示检测到损坏的擦除编码数据片段。	"ECOC：损坏的擦除编码数据片段"
ETAF	安全身份验证失败：使用传输层安全 (TLS) 的连接尝试失败。	"ETAF：安全身份验证失败"
GNRG	${post_edited_translations.segment}	"GNRG: GNDS注册"
GNUR	GNDS注销：服务已从StorageGRID系统中注销。	"GNUR：GNDS 注销"
GTED	网格任务已结束：CMN 服务已完成处理网格任务。	"GTED：网格任务已结束"
GTST	网格任务已启动：CMN 服务已开始处理网格任务。	"${post_edited_translations.segment}"
GTSU	已提交网格任务：已将网格任务提交到 CMN 服务。	"GTSU：网格任务已提交"
LLST	${post_edited_translations.segment}	"LLST：位置丢失"
OLST	对象丢失：无法在 StorageGRID 系统中找到请求的对象。	"OLST：系统检测到丢失对象"
SADD	安全审核禁用：已关闭审核消息日志记录。	"SADD：安全审核禁用"
${post_edited_translations.segment}	安全审核启用：已还原审核消息日志记录。	"SADE：启用安全审计"
SVRF	对象存储验证失败：内容块验证检查失败。	"SVRF：对象存储验证失败"
SVRU	对象存储验证未知：在对象存储中检测到意外的对象数据。	"SVRU：对象存储验证未知"
SYSD	${post_edited_translations.segment}	"SYSD：节点停止"

代码	消息标题和描述	请参见
SYST	节点停止：服务已启动正常停止。	"SYST：节点停止"
SYSU	节点启动：服务已启动；消息中显示了上一次关闭的性质。	"SYSU：节点启动"

StorageGRID 中对象存储事件的审核消息

属于对象存储审核类别的审核消息用于与 StorageGRID 系统中对象的存储和管理相关的事件。这些包括对象存储和检索、网格节点到网格节点的传输以及验证。

审核代码将随功能弃用而从产品和文档中删除。如果您遇到此处未列出的审核代码，请查看本主题的早期版本以获取较旧的 SG 版本信息。例如， "StorageGRID 11.8 对象存储审核消息"。

代码	问题描述	请参见
BROR	存储区只读请求：存储区进入或退出只读模式。	"BROR：Bucket 只读请求"
CBSE	对象发送结束：源实体完成了从网格节点到网格节点的数据传输操作。	"CBSE：对象发送结束"
CBRE	对象接收结束：目标实体完成了网格节点到网格节点的数据传输操作。	"CBRE：对象接收端"
CGRR	跨网格复制请求：StorageGRID 尝试进行跨网格复制操作，以在网格联合连接中的存储桶之间复制对象。	"CGRR：跨网格复制请求"
EBDL	空存储桶删除：ILM 扫描程序删除了一个存储桶中的对象，该存储桶正在删除所有对象（执行清空存储桶操作）。	"EBDL：空桶删除"
${post_edited_translations.segment}	空桶请求：用户发送了打开或关闭清空存储桶的请求（即删除存储桶对象或停止删除对象）。	"EBKR：空存储桶请求"
${post_edited_translations.segment}	${post_edited_translations.segment}	"${post_edited_translations.segment}"
${post_edited_translations.segment}	对象存储删除：内容块已从网格节点中删除，无法再直接请求。	"SREM：对象存储删除"

StorageGRID 中客户端读取操作的审核消息

当 S3 客户端应用程序请求检索对象时，将记录客户端读取审核消息。

代码	问题描述	使用者	请参见
S3SL	S3 Select 请求：记录 S3 Select 请求返回到客户端后的完成情况。S3SL 消息可以包括错误消息和错误代码详细信息。请求可能未成功。	S3客户端	"S3SL: S3 Select 请求"
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。 注意： 如果事务在子资源上操作，则审核消息将包括字段 S3SR。	S3客户端	"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。	S3客户端	"SHEA: S3 HEAD"

StorageGRID 中客户端写入操作的审核消息

当 S3 客户端应用程序请求创建或修改对象时，将记录客户端写入审核消息。

代码	问题描述	使用者	请参见
OVWR	对象覆盖：记录事务以用另一个对象覆盖一个对象。	S3客户端	"OVWR：对象覆盖"
SDEL	S3 DELETE：记录成功删除对象或存储桶的事务。 注意： 如果事务在子资源上操作，则审核消息将包括字段 S3SR。	S3客户端	"SDEL：S3 DELETE"
SPOS	S3 POST：记录成功的事务以将对象从 AWS Glacier 存储还原到 Cloud Storage Pool。	S3客户端	"SPOS：S3 POST"
SPUT	S3 PUT：记录成功的事务以创建新对象或存储桶。 注意： 如果事务在子资源上操作，则审核消息将包括字段 S3SR。	S3客户端	"SPUT：S3 PUT"
SUPD	S3 Metadata Updated：记录成功更新现有对象或存储桶元数据的事务。	S3客户端	"SUPD：S3 元数据已更新"

StorageGRID 管理审核消息

"管理"类别将用户请求记录到管理 API。

代码	消息标题和描述	请参见
${post_edited_translations.segment}	Management API 审核消息：用户请求的日志。	"${post_edited_translations.segment}"

StorageGRID ILM 审核消息

属于 ILM 审计类别的审核消息用于与信息生命周期管理 (ILM) 操作相关的事件。

代码	消息标题和描述	请参见
IDEL	ILM Initiated Delete：此审核消息在 ILM 开始删除对象的过程时生成。	"IDEL：ILM Initiated Delete"
LKCU	覆盖的对象清理。自动删除覆盖的对象以释放存储空间时会生成此审核消息。	"LKCU：覆盖对象清理"
ORLM	符合对象规则：此审核消息在按照 ILM 规则指定存储对象数据时生成。	"ORLM：Object Rules Met"

审核消息参考

StorageGRID 中存储桶只读请求的 BROR 审核消息

当存储区进入或退出只读模式时，LDR 服务会生成此审核消息。例如，在删除所有对象时，存储区进入只读模式。

代码	字段	问题描述
BKHD	存储桶 UUID	存储桶 ID。
BROV	存储区只读请求值	存储桶是否处于只读状态或正在退出只读状态（1 = 只读，0 = 非只读）。
BROS	存储桶只读原因	存储区被设为只读或离开只读状态的原因。例如，emptyBucket。
S3AI	S3租户帐户ID	发送请求的租户帐户的 ID。空值表示匿名访问。
S3BK	S3 存储分段	S3 存储桶名称。

StorageGRID 中对象接收开始的 CBRB 审核消息

在正常系统运行期间，随着数据的访问、复制和保留，内容块在不同节点之间不断传输。当从一个节点向另一个节点传输内容块时，此消息由目标实体发出。

代码	字段	问题描述
CNID	连接标识符	节点到节点会话/连接的唯一标识符。
CBID	内容块标识符	正在传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉取启动： 推送：此传输操作是由发送实体请求的。 PULL：接收实体请求此传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID。
CTDS	目标实体	CBID 传输的目的地（接收方）的节点 ID。
CTSS	开始序列计数	指示请求的第一个序列计数。如果成功，传输将从此序列计数开始。
CTES	预期结束序列计数	指示请求的最后一个序列计数。如果成功，则在接收到此序列计数时认为传输已完成。
RSLT	传输开始状态	传输开始时的状态： SUCS：已成功开始传输。

此审核消息表示在单个内容上启动了节点到节点的数据传输操作，由其内容块标识符标识。操作请求从"Start Sequence Count"到"Expected End Sequence Count"的数据。发送和接收节点由其节点 ID 标识。此信息可用于跟踪系统数据流，并与存储审计消息相结合，以验证副本计数。

StorageGRID 中对象接收结束的 **CBRE** 审核消息

当从一个节点到另一个节点的内容块传输完成时，此消息由目标实体发出。

代码	字段	问题描述
CNID	连接标识符	节点到节点会话/连接的唯一标识符。
CBID	内容块标识符	正在传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉取启动： 推送：此传输操作是由发送实体请求的。 PULL：接收实体请求此传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID。

代码	字段	问题描述
CTDS	目标实体	CBID 传输的目的地（接收方）的节点 ID。
CTSS	开始序列计数	指示开始传输的序列计数。
CTAS	实际结束序列计数	指示上次成功传输的序列计数。如果实际结束序列计数与开始序列计数相同，且传输结果不成功，则未交换任何数据。
RSLT	传输结果	传输操作的结果（从发送实体的角度）： SUCS：已成功完成传输；已发送所有请求的序列计数。 CONL：传输过程中连接丢失 CTMO：建立或传输期间连接超时 UNRE：目标节点 ID 无法访问 CRPT：由于接收到损坏或无效的数据而终止传输

此审核消息表示节点到节点的数据传输操作已完成。如果传输结果成功，则操作将数据从"开始序列计数"传输到"实际结束序列计数"。发送和接收节点由其节点 ID 标识。此信息可用于跟踪系统数据流并定位、制表和分析错误。与存储审核消息结合使用时，还可用于验证副本计数。

StorageGRID 中对象发送开始的 **CBSB** 审核消息

在正常系统运行期间，随着数据的访问、复制和保留，内容块在不同节点之间不断传输。当从一个节点向另一个节点传输内容块时，此消息由源实体发出。

代码	字段	问题描述
CNID	连接标识符	节点到节点会话/连接的唯一标识符。
CBID	内容块标识符	正在传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉取启动： 推送：此传输操作是由发送实体请求的。 PULL：接收实体请求此传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID。
CTDS	目标实体	CBID 传输的目的地（接收方）的节点 ID。
CTSS	开始序列计数	指示请求的第一个序列计数。如果成功，传输将从此序列计数开始。

代码	字段	问题描述
CTES	预期结束序列计数	指示请求的最后一个序列计数。如果成功，则在接收到此序列计数时认为传输已完成。
RSLT	传输开始状态	传输开始时的状态： SUCS：已成功开始传输。

此审核消息表示在单个内容上启动了节点到节点的数据传输操作，由其内容块标识符标识。操作请求从"Start Sequence Count"到"Expected End Sequence Count"的数据。发送和接收节点由其节点 ID 标识。此信息可用于跟踪系统数据流，并与存储审计消息相结合，以验证副本计数。

StorageGRID 中对象发送结束的 **CBSE** 审核消息

当内容块从一个节点转移到另一个节点的操作完成时，源实体将发出此消息。

代码	字段	问题描述
CNID	连接标识符	节点到节点会话/连接的唯一标识符。
CBID	内容块标识符	正在传输的内容块的唯一标识符。
CTDR	传输方向	指示 CBID 传输是推送启动还是拉取启动： 推送：此传输操作是由发送实体请求的。 PULL：接收实体请求此传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID。
CTDS	目标实体	CBID 传输的目的地（接收方）的节点 ID。
CTSS	开始序列计数	指示开始传输的序列计数。
CTAS	实际结束序列计数	指示上次成功传输的序列计数。如果实际结束序列计数与开始序列计数相同，且传输结果不成功，则未交换任何数据。

代码	字段	问题描述
RSLT	传输结果	传输操作的结果（从发送实体的角度）： SUCS：已成功完成传输；已发送所有请求的序列计数。 CONL：传输过程中连接丢失 CTMO：建立或传输期间连接超时 UNRE：目标节点 ID 无法访问 CRPT：由于接收到损坏或无效的数据而终止传输

此审核消息表示节点到节点的数据传输操作已完成。如果传输结果成功，则操作将数据从"开始序列计数"传输到"实际结束序列计数"。发送和接收节点由其节点 ID 标识。此信息可用于跟踪系统数据流并定位、制表和分析错误。与存储审核消息结合使用时，还可用于验证副本计数。

StorageGRID 中跨网格复制请求的 **CGRR** 审核消息

当 StorageGRID 尝试跨网格复制操作以在网格联合连接中的存储桶之间复制对象时，将生成此消息。

代码	字段	问题描述
CSIZ	对象大小	对象的大小（以字节为单位）。 CSIZ 属性已在 StorageGRID 11.8 中引入。因此，跨 StorageGRID 11.7 到 11.8 升级的跨网格复制请求的总对象大小可能不准确。
S3AI	S3租户帐户ID	拥有从中复制对象的存储桶的租户帐户的 ID。
GFID	网格联合连接 ID	用于跨网格复制的网格联合连接的 ID。
OPER	CGR操作	尝试的跨网格复制操作类型： • 0 = 复制对象 • 1 = 复制多部分对象 • 2 = 复制删除标记
S3BK	S3 存储分段	S3 存储桶名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。
VSID	版本 ID	正在复制的对象的特定版本的版本 ID。

代码	字段	问题描述
RSLT	结果代码	返回成功(SUCS)或一般错误(GERR)。

StorageGRID 中空存储桶对象删除的 **EBDL** 审核消息

ILM 扫描程序删除了一个存储桶中的对象，该存储桶正在删除所有对象（执行清空存储桶操作）。

代码	字段	问题描述
CSIZ	对象大小	对象的大小（以字节为单位）。
路径	S3 存储桶/键	S3 存储桶名称和 S3 密钥名称。
SEGC	容器UUID	分段对象的容器的 UUID。此值仅在对象已分段时可用。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
RSLT	删除操作的结果	事件、流程或事务的结果。如果与消息无关，则使用 NONE 而不是 SUCS，以免意外过滤消息。

StorageGRID 中空存储桶请求的 **EBKR** 审核消息

此消息表示用户发送了打开或关闭空存储桶的请求（即删除存储桶对象或停止删除对象）。

代码	字段	问题描述
BUID	存储桶 UUID	存储桶 ID。
EBJS	空的 Bucket JSON 配置	包含表示当前 Empty Bucket 配置的 JSON。
S3AI	S3租户帐户ID	发送请求的用户的租户帐户 ID。空值表示匿名访问。
S3BK	S3 存储桶	S3 存储桶名称。

StorageGRID 中缺失纠删码数据的 **ECMC** 审计消息

此审核消息指示系统检测到缺失的擦除编码数据片段。

代码	字段	问题描述
VCMC	VCS ID	包含丢失区块的VCS的名称。

代码	字段	问题描述
MCID	区块ID	缺少的擦除编码片段的标识符。
RSLT	结果	此字段的值为"NONE"。RSLT 是必填消息字段，但与此特定消息无关。使用"NONE"而不是"SUCS"，因此不会过滤此消息。

StorageGRID 中损坏的纠删编码数据的 **ECOC** 审核消息

此审核消息指示系统已检测到损坏的擦除编码数据片段。

代码	字段	问题描述
VCCO	VCS ID	包含损坏区块的 VCS 的名称。
VLID	Volume ID	包含损坏的纠删编码片段的 RangeDB 卷。
CCID	区块ID	损坏的擦除编码片段的标识符。
RSLT	结果	此字段的值为"NONE"。RSLT 是必填消息字段，但与此特定消息无关。使用"NONE"而不是"SUCS"，因此不会过滤此消息。

StorageGRID 中安全身份验证失败的 **ETAF** 审核消息

当使用传输层安全性 (TLS) 的连接尝试失败时，将生成此消息。

代码	字段	问题描述
CNID	连接标识符	身份验证失败的 TCP/IP 连接的唯一系统标识符。
RUID	用户身份	表示远程用户标识的服务相关标识符。

代码	字段	问题描述
RSLT	原因代码	故障原因： SCNI：安全连接建立失败。 CERM：证书缺失。 CERT：证书无效。 CERE：证书已过期。 CERR：证书已被吊销。 CSGN：证书签名无效。 CSGU：证书签名者未知。 UCRM：用户凭据缺失。 UCRI：用户凭据无效。 UCRU：不允许使用用户凭据。 TOUT：身份验证超时。

建立与使用 TLS 的安全服务的连接后，将使用 TLS 配置文件和内置于服务中的其他逻辑来验证远程实体的凭据。如果此身份验证由于无效、意外或不允许的证书或凭据而失败，则会记录审核消息。这样可以查询未经授权的访问尝试和其他与安全相关的连接问题。

该消息可能源于远程实体配置不正确，或者源于尝试向系统呈现无效或不允许的凭据。应监控此审核消息，以检测尝试获取对系统的未经授权访问的行为。

StorageGRID 中 **GNDS** 注册的 **GNRG** 审核消息

当服务在 StorageGRID 系统中更新或注册了有关自身的信息时，CMN 服务会生成此审核消息。

代码	字段	问题描述
RSLT	结果	更新请求的结果： • SUCS：成功 • SUNV：服务不可用 • GERR：其他故障
GNID	节点 ID	启动更新请求的服务的节点 ID。
GNTP	设备类型	网格节点的设备类型（例如，LDR 服务的 BLDR）。

代码	字段	问题描述
GNDV	设备型号版本	标识 DMDL 捆绑包中网格节点的设备模型版本的字符串。
GNGP	组	网格节点所属的组（在链接成本和服务查询排名的上下文中）。
GNIA	IP 地址	网格节点的 IP 地址。

每当网格节点更新其在网格节点捆绑包中的条目时，都会生成此消息。

StorageGRID 中 **GNDS** 注销的 **GNUR** 审核消息

当服务从 StorageGRID 系统注销其自身相关信息时，CMN 服务将生成此审核消息。

代码	字段	问题描述
RSLT	结果	更新请求的结果： • SUCS：成功 • SUNV：服务不可用 • GERR：其他故障
GNID	节点 ID	启动更新请求的服务的节点 ID。

StorageGRID 中已结束网格任务的 **GTED** 审核消息

此审核消息指示 CMN 服务已完成处理指定的网格任务并将任务移至历史表。如果结果为 SUCS、ABRT 或 ROLF，则会出现相应的 Grid Task Started 审核消息。其他结果表明，此网格任务的处理从未开始。

代码	字段	问题描述
TSID	任务 ID	此字段唯一标识生成的网格任务，并允许在其生命周期内管理网格任务。 注意： 任务 ID 在生成网格任务时分配，而不是在提交网格任务时分配。给定的网格任务可以多次提交，在这种情况下，"任务 ID"字段不足以唯一链接"已提交"、"已开始"和"已结束"审核消息。

代码	字段	问题描述
RSLT	结果	网格任务的最终状态结果： • SUCS：已成功完成网格任务。 • ABRT：网格任务已终止，没有回滚错误。 • ROLF：网格任务已终止，无法完成回滚过程。 • CANC：网格任务在启动前已被用户取消。 • EXPR:网格任务在启动前已过期。 • IVLD：网格任务无效。 • AUTH：网格任务未授权。 • DUPL：网格任务因重复而被拒绝。

StorageGRID 中已启动网格任务的 **GTST** 审核消息

此审计消息指示 CMN 服务已开始处理指定的网格任务。对于由内部网格任务提交服务启动并选择自动激活的网格任务，审计消息紧跟在网格任务提交消息之后。对于提交到"挂起"表的网格任务，此消息在用户启动网格任务时生成。

代码	字段	问题描述
TSID	任务 ID	此字段唯一标识生成的网格任务，并允许在其生命周期内管理任务。 注意： 任务 ID 在生成网格任务时分配，而不是在提交网格任务时分配。给定的网格任务可以多次提交，在这种情况下，"任务 ID"字段不足以唯一链接"已提交"、"已开始"和"已结束"审核消息。
RSLT	结果	结果。此字段只有一个值： • SUCS：已成功启动网格任务。

StorageGRID 中已提交网格任务的 **GTSU** 审核消息

此审核消息表示已将网格任务提交到 CMN 服务。

代码	字段	问题描述
TSID	任务 ID	唯一标识生成的网格任务，并允许在其生命周期内管理任务。 注意： 任务 ID 在生成网格任务时分配，而不是在提交网格任务时分配。给定的网格任务可以多次提交，在这种情况下，"任务 ID"字段不足以唯一链接"已提交"、"已开始"和"已结束"审核消息。
TTYP	任务类型	网格任务的类型。

代码	字段	问题描述
TVER	任务版本	表示网格任务版本的数字。
TDSC	任务说明	网格任务的人工可读说明。
VATS	在时间戳之后有效	网格任务有效的最早时间（从 1970 年 1 月 1 日起的 UINT64 微秒 - UNIX 时间）。
VBTS	有效期截止时间戳	网格任务有效的最新时间（从 1970 年 1 月 1 日起的 UINT64 微秒 - UNIX 时间）。
TSRC	源	任务的源： • TXTB：网格任务通过 StorageGRID 系统作为签名文本块提交。 • 网格：网格任务已通过内部网格任务提交服务提交。
ACTV	激活类型	激活类型： • AUTO: 网格任务已提交以进行自动激活。 • PEND：网格任务已提交到挂起表中。这是 TXTB 源唯一的可能性。
RSLT	结果	提交结果： • SUCS：网格任务已成功提交。 • 失败：此任务已直接移至历史记录表。

StorageGRID 中 **ILM** 启动删除的 **IDEL** 审核消息

此消息在 ILM 开始删除对象的过程时生成。

在以下任何一种情况下都会生成IDEL消息：

- 对于合规 **S3** 存储桶中的对象：当 ILM 开始自动删除对象的过程时，会生成此消息，因为其保留期已过期（假设已启用自动删除设置且法律保留已关闭）。
- 对于不合规 **S3** 存储桶中的对象。此消息在 ILM 开始删除对象的过程时生成，因为当前活动 ILM 策略中没有放置指令适用于该对象。

代码	字段	问题描述
CBID	内容块标识符	对象的CBID。
${post_edited_translations.segment}	${post_edited_translations.segment}	仅适用于合规 S3 存储桶中的对象。0（false）或 1（true），表示合规对象的保留期结束时是否应自动删除，除非存储桶处于合法冻结状态。

代码	字段	问题描述
CMPL	合规性：法律保留	仅适用于合规 S3 存储桶中的对象。0 (false) 或 1 (true)，指示存储桶当前是否处于合法冻结状态。
CMPR	合规性：保留期限	仅适用于合规 S3 存储桶中的对象。对象保留期的长度（以分钟为单位）。
CTME	合规性：采集时间	仅适用于合规 S3 存储桶中的对象。对象的摄取时间。您可以将保留期（以分钟为单位）添加到此值，以确定何时可以从存储桶中删除对象。
DMRK	删除标记版本 ID	从版本化存储桶中删除对象时创建的删除标记的版本 ID。存储桶上的操作不包括此字段。
CSIZ	内容大小	对象的大小（以字节为单位）。
LOCS	位置	对象数据在 StorageGRID 系统中的存储位置。如果对象没有位置（例如，它已被删除），则 LOCS 的值为""。 CLEC：对于纠删码对象，应用于对象数据的纠删码配置文件 ID 和纠删码组 ID。 CLDI：对于复制对象，LDR 节点 ID 和对象位置的卷 ID。 CLNL：如果对象数据已存档，则为对象位置的 ARC 节点 ID。
路径	S3 存储桶/键	S3 存储桶名称和 S3 密钥名称。
RSLT	结果	ILM 操作的结果。 SUCS：ILM 操作成功。
规则	规则标签	• 如果合规 S3 存储桶中的对象由于其保留期已过期而被自动删除，则此字段为空。 • 如果由于当前没有适用于该对象的放置指令而正在删除该对象，则此字段显示最后一个适用于该对象的 ILM 规则的可读标签。
SGRP	站点（组）	如果存在，则对象已在指定站点被删除，该站点不是接收对象的站点。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	已删除对象的特定版本的版本 ID。未版本化存储桶中存储桶和对象的操作不包括此字段。

StorageGRID 中覆盖对象清理的 **LKCU** 审核消息

此消息是在 StorageGRID 删除先前需要清理以释放存储空间的已覆盖对象时生成的。当 S3 客户端将对象写入已包含对象的路径时，对象将被覆盖。删除过程会自动在后台执行。

代码	字段	问题描述
CSIZ	内容大小	对象的大小（以字节为单位）。
LTYP	清理类型	仅供内部使用。
LUID	已删除对象 UUID	已删除的对象的标识符。
路径	S3 存储桶/键	S3 存储桶名称和 S3 密钥名称。
SEGC	容器UUID	分段对象的容器的 UUID。此值仅在对象已分段时可用。
UUID	通用唯一标识符	仍然存在的对象的标识符。此值仅在对象未被删除时可用。

StorageGRID 中泄漏对象清理的 **LKDM** 审计消息

当已清理或删除泄漏的区块时，将生成此消息。区块可以是复制对象或擦除编码对象的一部分。

代码	字段	问题描述
CLOC	区块位置	已删除的已泄露区块的文件路径。

CTYP	区块类型	区块类型：
		
		`ec: Erasure-coded object chunk`
		
		`repl: Replicated object chunk`

代码	字段	问题描述

LTYP	泄漏类型	可检测到的五种泄漏类型：
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

CTIM	区块创建时间	创建泄漏块的时间。
UUID	通用唯一标识符	${post_edited_translations.segment}
CBID	内容块标识符	泄漏区块所属对象的 CBID。
CSIZ	内容大小	区块的大小（以字节为单位）。

StorageGRID 中丢失对象副本位置的 **LLST** 审核消息

每当找不到对象副本（复制或擦除编码）的位置时，都会生成此消息。

代码	字段	问题描述
CBIL	CBID	受影响的CBID。
ECPR	纠删码配置文件	用于擦除编码对象数据。使用的擦除编码配置文件的 ID。
LTYP	位置类型	CLDI（在线）：用于复制对象数据 CLEC（在线）：用于擦除编码对象数据 CLNL（近线）：用于已存档的复制对象数据
NOID	源节点 ID	丢失位置的节点 ID。

代码	字段	问题描述
PCLD	复制对象的路径	丢失对象数据的磁盘位置的完整路径。仅当 LTYP 的值为 CLDI 时（即对于复制对象）才返回。 格式为 `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	结果	始终为 NONE。RSLT 是必填消息字段，但与此消息无关。使用 NONE 而不是 SUCS，因此不会过滤此消息。
TSRC	触发源	USER: 用户已触发 SYST：系统触发
UUID	通用唯一ID	${post_edited_translations.segment}

StorageGRID 中管理 **API** 请求的 **MGAU** 审核消息

管理类别将用户请求记录到 Management API。每个向有效 API URI 发出的非 GET 或 HEAD 的 HTTP 请求都会记录包含用户名、IP 和 API 请求类型的响应。无效的 API URI（如 /api/v3-authorize）以及向有效 API URI 发出的无效请求不会被记录。

代码	字段	问题描述
MDIP	目标 IP 地址	服务器（目标）IP 地址。
MDNA	域名	主机域名。
${post_edited_translations.segment}	请求路径	请求路径。
MPQP	请求查询参数	请求的查询参数。
MRBD	请求正文	请求正文的内容。默认情况下会记录响应正文，但在某些情况下，当响应正文为空时，会记录请求正文。由于响应正文中没有以下信息，因此它是从以下 POST 方法的请求正文中获取的： • **POST authorize** 中的用户名和帐户 ID • **POST /grid/grid-networks/update** 中的新子网配置 • **POST /grid/ntp-servers/update** 中的新 NTP 服务器 • **POST /grid/servers/decommission** 中已停用的服务器 ID 注意： 敏感信息将被删除（例如 S3 访问密钥）或用星号掩盖（例如密码）。

代码	字段	问题描述
${post_edited_translations.segment}	请求方法	${post_edited_translations.segment} • POST • PUT • DELETE • PATCH
MRSC	响应代码	${post_edited_translations.segment}
MRSP	响应正文	默认情况下会记录响应的内容（响应正文）。 注意： 敏感信息将被删除（例如 S3 访问密钥）或用星号掩盖（例如密码）。
MSIP	${post_edited_translations.segment}	客户端（源） IP 地址。
MUUN	用户 URN	发送请求的用户的 URN（统一资源名称）。
RSLT	结果	返回成功(SUCS)或后端报告的错误。

StorageGRID 中系统检测到丢失对象的 **OLST** 审核消息

当 DDS 服务无法在 StorageGRID 系统中找到任何对象副本时，将生成此消息。

代码	字段	问题描述
CBID	内容块标识符	丢失对象的 CBID。
NOID	节点 ID	如果可用，则为丢失对象的最后已知直接或近线位置。如果卷信息不可用，则可以仅具有无卷 ID 的节点 ID。
路径	S3 存储桶/键	如果有，请提供 S3 存储桶名称和 S3 密钥名称。
RSLT	结果	此字段的值为 NONE。RSLT 是必填消息字段，但与此消息无关。使用 NONE 而不是 SUCS，以确保此消息不会被过滤。
UUID	通用唯一ID	StorageGRID 系统中丢失对象的标识符。
VOLI	Volume ID	如果可用，则为丢失对象的最后已知位置的存储节点的卷 ID。

StorageGRID 中满足 **ILM** 规则的 **ORLM** 审核消息

${post_edited_translations.segment}

如果策略中的其他规则使用"对象大小"高级筛选器，则根据默认的"生成 2 个副本"规则成功存储对象时，不会生成 ORLM 消息。

代码	字段	问题描述
BUID	${post_edited_translations.segment}	Bucket ID 字段。用于内部操作。仅在 STAT 为 PRGD 时出现。
CBID	内容块标识符	对象的CBID。
CSIZ	内容大小	对象的大小（以字节为单位）。
LOCS	位置	对象数据在 StorageGRID 系统中的存储位置。如果对象没有位置（例如，它已被删除），则 LOCS 的值为"。 CLEC：对于纠删码对象，应用于对象数据的纠删码配置文件 ID 和纠删码组 ID。 CLDI：对于复制对象，LDR 节点 ID 和对象位置的卷 ID。 CLNL：如果对象数据已存档，则为对象位置的 ARC 节点 ID。
路径	S3 存储桶/键	S3 存储桶名称和 S3 密钥名称。
RSLT	结果	ILM 操作的结果。 SUCS：ILM 操作成功。
规则	规则标签	${post_edited_translations.segment}
SEGC	容器UUID	分段对象的容器的 UUID。此值仅在对象已分段时可用。
${post_edited_translations.segment}	容器 CBID	分段对象的容器的 CBID。此值仅适用于分段和多部分对象。

代码	字段	问题描述
STAT	状态	ILM 操作的状态。 完成：针对对象的 ILM 操作已完成。 DFER：此对象已标记为将来的 ILM 重新评估。 PRGD：已从 StorageGRID 系统中删除此对象。 NLOC：无法再在 StorageGRID 系统中找到对象数据。此状态可能表示对象数据的所有副本都丢失或损坏。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	在版本化存储桶中创建的新对象的版本 ID。对未版本化存储桶中的存储桶和对象的操作不包括此字段。

可以为单个对象多次发出 ORLM 审核消息。例如，每当发生以下事件之一时，就会发出此通知：

- 永远满足对象的 ILM 规则。
- 此纪元满足对象的 ILM 规则。
- ILM规则已删除该对象。
- 后台验证过程检测到已复制对象数据的副本已损坏。StorageGRID 系统执行 ILM 评估以替换损坏的对象。

相关信息

- "对象摄取事务"
- "对象删除事务"

StorageGRID 中对象覆写的 **OVWR** 审核消息

当外部（客户端请求）操作导致一个对象被另一个对象覆盖时，会生成此消息。

代码	字段	问题描述
CBID	内容块标识符（新增）	新对象的CBID。
CSIZ	上一个对象大小	要覆盖的对象的大小（以字节为单位）。
OCBD	内容块标识符（上一个）	上一个对象的CBID。
UUID	通用唯一ID (新增)	StorageGRID 系统中新对象的标识符。

代码	字段	问题描述
OUID	通用唯一 ID（以前）	StorageGRID 系统中上一个对象的标识符。
路径	S3 对象路径	用于上一个对象和新对象的S3对象路径
RSLT	结果代码	对象覆盖事务的结果。结果始终为： SUCS：成功
SGRP	站点（组）	如果存在，则在指定站点上删除被覆盖的对象，该站点不是接收被覆盖对象的站点。

StorageGRID 中 **S3 Select** 请求的 **S3SL** 审核消息

此消息记录 S3 Select 请求返回到客户端后的完成情况。S3SL 消息可以包括错误消息和错误代码详细信息。请求可能未成功。

代码	字段	问题描述
BYSC	扫描的字节数	从存储节点扫描（接收）的字节数。 如果对象被压缩，BYSC 和 BYPR 可能不同。如果对象被压缩，BYSC 将包含压缩字节数，BYPR 将是解压缩后的字节数。
BYPR	已处理字节数	已处理的字节数。指示 S3 Select 作业实际处理或操作的"Bytes Scanned"字节数。
BYRT	返回的字节数	S3 Select 作业返回到客户端的字节数。
REPR	已处理的记录	S3 Select 作业从存储节点接收的记录或行数。
RERT	返回的记录	S3 Select 作业返回到客户端的记录或行数。
JOFI	作业已完成	指示 S3 Select 作业是否已完成处理。如果为 false，则作业无法完成，错误字段可能包含数据。客户端可能收到了部分结果，或者根本没有结果。
REID	请求 ID	S3 Select 请求的标识符。
EXTM	执行时间	S3 Select 作业完成所需的时间（以秒为单位）。
ERMG	错误消息	S3 Select 作业生成的错误消息。

代码	字段	问题描述
ERTY	错误类型	S3 Select 作业生成的错误类型。
ERST	错误堆栈跟踪	S3 Select 作业生成的错误堆栈跟踪。
S3BK	S3 存储分段	S3 存储桶名称。
S3AK	S3 访问密钥 ID（请求发送方）	发送请求的用户的 S3 访问密钥 ID。
S3AI	S3 租户账号 ID（请求发送方）	发送请求的用户的租户帐户 ID。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。

StorageGRID 中安全审核禁用的 **SADD** 审核消息

此消息指示原始服务（节点 ID）已关闭审核消息日志记录。StorageGRID 不再收集或传递审核消息。

代码	字段	问题描述
AETM	启用方法	用于禁用审核的方法。
AEUN	用户名	执行命令以禁用审核日志记录的用户名。
RSLT	结果	此字段的值为 NONE。RSLT 是必填消息字段，但与此消息无关。使用 NONE 而不是 SUCS，以确保此消息不会被过滤。

该消息暗示日志记录以前已启用，但现在已被禁用。这通常仅在批量摄取时使用，以提高系统性能。在批量活动之后，将恢复审核（SADE），然后永久阻止禁用审核的功能。

StorageGRID 中启用安全审核的 **SADE** 审核消息

此消息指示发起服务（节点 ID）已恢复审核消息日志记录。StorageGRID 再次收集和传递审核消息。

代码	字段	问题描述
AETM	启用方法	用于启用审核的方法。
AEUN	用户名	执行命令以启用审核日志记录的用户名。

代码	字段	问题描述
RSLT	结果	此字段的值为 NONE。RSLT 是必填消息字段，但与此消息无关。使用 NONE 而不是 SUCS，以确保此消息不会被过滤。

该消息暗示日志记录以前被禁用（SADD），但现在已恢复。这通常仅用于批量载入以提高系统性能。在批量活动之后，将恢复审核，然后永久阻止禁用审核的功能。

StorageGRID 中对象存储提交的 **SCMT** 审核消息

在提交之前（即持久存储之前），网格内容不会被提供或识别为已存储。持久存储的内容已完全写入磁盘，并通过了相关的完整性检查。当内容块提交到存储时，将发出此消息。

代码	字段	问题描述
CBID	内容块标识符	提交给永久存储的内容块的唯一标识符。
RSLT	结果代码	对象存储到磁盘时的状态： SUCS: 对象已成功存储。

此消息表示给定的内容块已完全存储和验证，现在可以请求。它可用于跟踪系统内的数据流。

StorageGRID 中 **S3 DELETE** 事务的 **SDEL** 审核消息

当 S3 客户端发出删除事务时，将发出删除指定对象或存储桶或删除存储桶/对象子资源的请求。如果事务成功，此消息将由服务器发出。

代码	字段	问题描述
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段设置为 0。存储桶上的操作不包括此字段。
CNCH	一致性控制标头	Consistency-Control HTTP 请求标头的值（如果存在于请求中）。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	已删除对象的大小（以字节为单位）。存储桶上的操作不包括此字段。
DMRK	删除标记版本 ID	从版本化存储桶中删除对象时创建的删除标记的版本 ID。存储桶上的操作不包括此字段。
GFID	网格联盟连接 ID	与跨网格复制删除请求关联的网格联合连接的连接 ID。仅包含在目标网格的审核日志中。

代码	字段	问题描述
GFSA	网格联盟源帐户 ID	跨网格复制删除请求的源网格上租户的帐户 ID。仅包含在目标网格的审核日志中。
HTRH	HTTP 请求标头	配置期间选择的已记录 HTTP 请求标头名称和值的列表。 `X-Forwarded-For` 如果请求中存在且 `X-Forwarded-For`值与请求发送方 IP 地址不同（SAIP 审核字段），则会自动包含。 x-amz-bypass-governance-retention 如果请求中存在该内容，则会自动包含在内。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，指示上次修改对象的时间。
RSLT	结果代码	DELETE 事务的结果。结果始终为： SUCS：成功
S3AI	S3 租户账号 ID（请求发送方）	发送请求的用户的租户帐户 ID。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发送方）	发送请求的用户的哈希 S3 访问密钥 ID。空值表示匿名访问。
S3BK	S3 存储桶	S3 存储桶名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。
S3SR	S3 子资源	正在对其进行操作的存储区或对象子资源（如适用）。
SACC	S3 租户帐户名称（请求发送方）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发送方）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3租户帐户名称（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
SBAI	S3 租户帐户 ID（存储区所有者）	目标存储桶所有者的租户帐户 ID。用于识别跨账户或匿名访问。

代码	字段	问题描述
SGRP	站点（组）	如果存在，则对象已在指定站点被删除，该站点不是接收对象的站点。
SUSR	S3 用户 URN（请求发送方）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户或 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间（微秒）。
TLIP	受信任的负载平衡器 IP 地址	如果请求由受信任的第 7 层负载均衡器路由，则为负载均衡器的 IP 地址。
UUDM	删除标记的通用唯一标识符	删除标记的标识符。审核日志消息指定 UUDM 或 UUID，其中 UUDM 表示由于对象删除请求而创建的删除标记，UUID 表示对象。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	已删除对象的特定版本的版本 ID。未版本化存储桶中存储桶和对象的操作不包括此字段。

StorageGRID 中 **S3 GET** 事务的 **SGET** 审核消息

当 S3 客户端发出 GET 事务时，将发出请求以检索对象或在存储桶中列出对象，或删除存储桶/对象子资源。如果事务成功，服务器将发出此消息。

代码	字段	问题描述
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段设置为 0。存储桶上的操作不包括此字段。
CNCH	一致性控制标头	Consistency-Control HTTP 请求标头的值（如果存在于请求中）。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储桶上的操作不包括此字段。
HTRH	HTTP 请求标头	配置期间选择的已记录 HTTP 请求标头名称和值的列表。 `X-Forwarded-For` 如果请求中存在且 `X-Forwarded-For`值与请求发送方 IP 地址不同（SAIP 审核字段），则会自动包含。

代码	字段	问题描述
LITY	ListObjectsV2	已请求 *v2 format* 响应。有关详细信息，请参见 "AWS ListObjectsV2"。仅适用于 GET bucket 操作。
NCHD	子项数量	包括密钥和常用前缀。仅适用于 GET bucket 操作。
RANG	范围读取	仅适用于范围读取操作。指示此请求读取的字节范围。斜杠（/）之后的值显示整个对象的大小。
RSLT	结果代码	GET 事务的结果。结果始终为： SUCS：成功
S3AI	S3 租户账号 ID（请求发送方）	发送请求的用户的租户帐户 ID。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发送方）	发送请求的用户的哈希 S3 访问密钥 ID。空值表示匿名访问。
S3BK	S3 存储桶	S3 存储桶名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。
S3SR	S3 子资源	正在对其进行操作的存储区或对象子资源（如适用）。
SACC	S3 租户帐户名称（请求发送方）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发送方）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3租户帐户名称（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
SBAI	S3 租户帐户 ID（存储区所有者）	目标存储桶所有者的租户帐户 ID。用于识别跨账户或匿名访问。
SUSR	S3 用户 URN（请求发送方）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户或 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。

代码	字段	问题描述
时间	时间	请求的总处理时间（微秒）。
TLIP	受信任的负载平衡器 IP 地址	如果请求由受信任的第 7 层负载均衡器路由，则为负载均衡器的 IP 地址。
TRNC	截断或未截断	如果返回所有结果，则设置为 false。如果有更多结果可返回，则设置为 true。仅适用于 GET bucket 操作。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	请求的对象的特定版本的版本 ID。未版本化存储桶中存储桶和对象的操作不包括此字段。

StorageGRID 中 **S3 HEAD** 操作的 **SHEA** 审核消息

当 S3 客户端发出 HEAD 操作时，会请求检查对象或存储桶是否存在并检索有关对象的元数据。如果操作成功，服务器将发出此消息。

代码	字段	问题描述
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段设置为 0。存储桶上的操作不包括此字段。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	选中对象的大小（以字节为单位）。存储桶上的操作不包括此字段。
HTRH	HTTP 请求标头	配置期间选择的已记录 HTTP 请求标头名称和值的列表。 `X-Forwarded-For` 如果请求中存在且 `X-Forwarded-For`值与请求发送方 IP 地址不同（SAIP 审核字段），则会自动包含。
RSLT	结果代码	GET 事务的结果。结果始终为： SUCS：成功
S3AI	S3 租户账号 ID（请求发送方）	发送请求的用户的租户帐户 ID。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发送方）	发送请求的用户的哈希 S3 访问密钥 ID。空值表示匿名访问。

代码	字段	问题描述
S3BK	S3 存储桶	S3 存储桶名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。
SACC	S3 租户帐户名称（请求发送方）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发送方）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3租户帐户名称（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
SBAI	S3 租户帐户 ID（存储区所有者）	目标存储桶所有者的租户帐户 ID。用于识别跨账户或匿名访问。
SUSR	S3 用户 URN（请求发送方）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户或 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间（微秒）。
TLIP	受信任的负载平衡器 IP 地址	如果请求由受信任的第 7 层负载均衡器路由，则为负载均衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	请求的对象的特定版本的版本 ID。未版本化存储桶中存储桶和对象的操作不包括此字段。

StorageGRID 中 **S3 POST** 事务的 **SPOS** 审核消息

当 S3 客户端发出 POST 对象请求时，如果事务成功，服务器将发出此消息。

代码	字段	问题描述
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段设置为 0。
CNCH	一致性控制标头	Consistency-Control HTTP 请求标头的值（如果存在于请求中）。

代码	字段	问题描述
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。
HTRH	HTTP 请求标头	配置期间选择的已记录 HTTP 请求标头名称和值的列表。 `X-Forwarded-For` 如果请求中存在且 `X-Forwarded-For`值与请求发送方 IP 地址不同（SAIP 审核字段），则会自动包含。 （不适用于SPOS）。
RSLT	结果代码	RestoreObject 请求的结果。结果始终为： SUCS：成功
S3AI	S3 租户账号 ID（请求发送方）	发送请求的用户的租户帐户 ID。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发送方）	发送请求的用户的哈希 S3 访问密钥 ID。空值表示匿名访问。
S3BK	S3 存储桶	S3 存储桶名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。
S3SR	S3 子资源	正在对其进行操作的存储区或对象子资源（如适用）。 对于 S3 Select 操作，设置为"select"。
SACC	S3 租户帐户名称（请求发送方）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发送方）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3租户帐户名称（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
SBAI	S3 租户帐户 ID（存储区所有者）	目标存储桶所有者的租户帐户 ID。用于识别跨账户或匿名访问。

代码	字段	问题描述
SRCF	子资源配置	还原信息。
SUSR	S3 用户 URN（请求发送方）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户或 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间（微秒）。
TLIP	受信任的负载平衡器 IP 地址	如果请求由受信任的第 7 层负载均衡器路由，则为负载均衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	请求的对象的特定版本的版本 ID。未版本化存储桶中存储桶和对象的操作不包括此字段。

StorageGRID 中 **S3 PUT** 事务的 **SPUT** 审核消息

当 S3 客户端发出 PUT 事务时，会请求创建新对象或存储桶，或删除存储桶/对象子资源。如果事务成功，此消息将由服务器发出。

代码	字段	问题描述
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段设置为 0。存储桶上的操作不包括此字段。
CMPS	合规性设置	创建存储桶时使用的合规性设置（如果存在于请求中）（截断为前 1024 个字符）。
CNCH	一致性控制标头	Consistency-Control HTTP 请求标头的值（如果存在于请求中）。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储桶上的操作不包括此字段。
GFID	网格联盟连接 ID	与跨网格复制 PUT 请求关联的网格联合连接的连接 ID。仅包含在目标网格的审核日志中。
GFSA	网格联盟源帐户 ID	跨网格复制 PUT 请求的源网格上租户的帐户 ID。仅包含在目标网格的审核日志中。

代码	字段	问题描述
HTRH	HTTP 请求标头	配置期间选择的已记录 HTTP 请求标头名称和值的列表。 `X-Forwarded-For` 如果请求中存在且 `X-Forwarded-For`值与请求发送方 IP 地址不同（SAIP 审核字段），则会自动包含。 x-amz-bypass-governance-retention 如果请求中存在该内容，则会自动包含在内。
LKEN	对象锁定已启用	请求标头的值 x-amz-bucket-object-lock-enabled（如果存在于请求中）。
LKLH	对象锁定法律保留	请求标头 `x-amz-object-lock-legal-hold`的值（如果存在于 PutObject 请求中）。
LKMD	对象锁定保留模式	请求标头 `x-amz-object-lock-mode`的值（如果存在于 PutObject 请求中）。
LKRU	对象锁定保留至日期	请求标头 `x-amz-object-lock-retain-until-date`的值（如果存在于 PutObject 请求中）。值限制在对象载入日期起 100 年以内。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，指示上次修改对象的时间。
RSLT	结果代码	PUT 事务的结果。结果始终为： SUCS：成功
S3AI	S3 租户账号 ID（请求发送方）	发送请求的用户的租户帐户 ID。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发送方）	发送请求的用户的哈希 S3 访问密钥 ID。空值表示匿名访问。
S3BK	S3 存储桶	S3 存储桶名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。
S3SR	S3 子资源	正在对其进行操作的存储区或对象子资源（如适用）。
SACC	S3 租户帐户名称（请求发送方）	发送请求的用户的租户帐户名称。匿名请求为空。

代码	字段	问题描述
SAIP	IP 地址（请求发送方）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3租户帐户名称（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
SBAI	S3 租户帐户 ID（存储区所有者）	目标存储桶所有者的租户帐户 ID。用于识别跨账户或匿名访问。
SRCF	子资源配置	新的子资源配置（截断为前 1024 个字符）。
SUSR	S3 用户 URN（请求发送方）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户或 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间（微秒）。
TLIP	受信任的负载平衡器 IP 地址	如果请求由受信任的第 7 层负载均衡器路由，则为负载均衡器的 IP 地址。
ULID	上传 ID	仅包含在 CompleteMultipartUpload 操作的 SPUT 消息中。表示所有分段已上传并组装完成。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	在版本化存储桶中创建的新对象的版本 ID。对未版本化存储桶中的存储桶和对象的操作不包括此字段。
VSST	版本控制状态	存储区的新版本控制状态。使用两种状态："已启用"或"已暂停"。对象上的操作不包括此字段。

StorageGRID 中对象存储删除的 **SREM** 审核消息

当内容从永久存储中删除且无法再通过常规 API 访问时，将发出此消息。

代码	字段	问题描述
CBID	内容块标识符	从永久存储中删除的内容块的唯一标识符。

代码	字段	问题描述
RSLT	结果代码	指示内容删除操作的结果。唯一定义的值是： SUCS：已从永久存储中删除内容

此审核消息表示给定的内容块已从节点中删除，无法再直接请求。该消息可用于跟踪系统内已删除内容的流动。

StorageGRID 中 **S3** 元数据更新的 **SUPD** 审核消息

当 S3 客户端更新已载入对象的元数据时，此消息由 S3 API 生成。如果元数据更新成功，则该消息由服务器发出。

代码	字段	问题描述
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段设置为 0。存储桶上的操作不包括此字段。
CNCH	一致性控制标头	更新存储桶的合规性设置时，Consistency-Control HTTP 请求标头的值（如果存在于请求中）。
CNID	连接标识符	TCP/IP 连接的唯一系统标识符。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。存储桶上的操作不包括此字段。
HTRH	HTTP 请求标头	配置期间选择的已记录 HTTP 请求标头名称和值的列表。 `X-Forwarded-For` 如果请求中存在且 `X-Forwarded-For`值与请求发送方 IP 地址不同（SAIP 审核字段），则会自动包含。
RSLT	结果代码	GET 事务的结果。结果始终为： SUCS：成功
S3AI	S3 租户账号 ID（请求发送方）	发送请求的用户的租户帐户 ID。空值表示匿名访问。
S3AK	S3 访问密钥 ID（请求发送方）	发送请求的用户的哈希 S3 访问密钥 ID。空值表示匿名访问。
S3BK	S3 存储桶	S3 存储桶名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储桶名称。存储桶上的操作不包括此字段。

代码	字段	问题描述
SACC	S3 租户帐户名称（请求发送方）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发送方）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3租户帐户名称（存储桶所有者）	存储桶所有者的租户帐户名称。用于识别跨账户或匿名访问。
SBAI	S3 租户帐户 ID（存储区所有者）	目标存储桶所有者的租户帐户 ID。用于识别跨账户或匿名访问。
SUSR	S3 用户 URN（请求发送方）	发出请求的用户的租户帐户 ID 和用户名。用户可以是本地用户或 LDAP 用户。例如： `urn:sgws:identity::03393893651506583485:root` 匿名请求为空。
时间	时间	请求的总处理时间（微秒）。
TLIP	受信任的负载平衡器 IP 地址	如果请求由受信任的第 7 层负载均衡器路由，则为负载均衡器的 IP 地址。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	已更新元数据的对象的特定版本的版本 ID。未版本化存储桶中存储桶和对象的操作不包括此字段。

StorageGRID 中对象存储验证失败的 **SVRF** 审核消息

每当内容块未通过验证过程时，都会显示此消息。每次从磁盘读取或写入复制对象数据时，都会执行多次验证和完整性检查，以确保发送给请求用户的数据与最初摄入系统的数据相同。如果任何这些检查失败，系统会自动隔离损坏的复制对象数据，以防止再次检索。

代码	字段	问题描述
CBID	内容块标识符	验证失败的内容块的唯一标识符。

代码	字段	问题描述
RSLT	结果代码	验证失败类型： CRCF：Cyclic redundancy check (CRC) 失败。 HMAC：基于哈希的消息验证码 (HMAC) 检查失败。 EHSH：意外的加密内容哈希。 PHSH：意外的原始内容哈希。 SEQC：磁盘上的数据序列不正确。 PERR：磁盘文件的结构无效。 DERR：磁盘错误。 FNAM：文件名错误。

应密切监控此消息。内容验证失败可能表明即将发生硬件故障。

要确定触发消息的操作，请参阅 AMID（模块 ID）字段的值。例如，SVFY 值表示消息是由存储验证器模块生成的，即后台验证，而 STOR 表示消息是由内容检索触发的。

StorageGRID 中未知对象存储内容的 **SVRU** 审核消息

LDR 服务的存储组件持续扫描对象存储中已复制对象数据的所有副本。当在对象存储中检测到已复制对象数据的未知或意外副本并将其移动到隔离目录时，将发出此消息。

代码	字段	问题描述
FPTH	文件路径	意外对象副本的文件路径。
RSLT	结果	此字段的值为"NONE"。RSLT 是必填消息字段，但与此消息无关。使用"NONE"而不是"SUCS"，因此不会过滤此消息。

应密切监控 SVRU：Object Store Verify Unknown 审核消息。这意味着在对象存储中检测到对象数据的意外副本。应立即调查这种情况，以确定这些副本是如何创建的，因为这可能表明硬件即将发生故障。

StorageGRID 中正常节点停止的 **SYSD** 审核消息

正常停止服务时，将生成此消息以指示请求关闭。通常，此消息仅在后续重新启动后发送，因为在关闭之前不会清除审核消息队列。如果服务尚未重新启动，请查找在关闭序列开始时发送的 SYST 消息。

代码	字段	问题描述
RSLT	正常关机	关闭的性质： SUCS：系统已正常关闭。

该消息不指示主机服务器是否正在停止，仅指示报告服务。SYSD 的 RSLT 不能指示"脏"关闭，因为消息仅由"干净"关闭生成。

StorageGRID 中节点停止的 **SYST** 审核消息

当服务正常停止时，将生成此消息以指示已请求关闭，并且该服务已启动其关闭序列。SYST 可用于在服务重新启动之前确定是否已请求关闭（与 SYSD 不同，SYSD 通常在服务重新启动后发送）。

代码	字段	问题描述
RSLT	正常关机	关闭的性质： SUCS：系统已正常关闭。

该消息不指示主机服务器是否正在停止，仅指示报告服务。SYST 消息的 RSLT 代码不能指示"脏"关闭，因为该消息仅由"干净"关闭生成。

节点的 **SYSU** 审核消息在 **StorageGRID** 中开始

当服务重新启动时，将生成此消息，以指示上一次关闭是正常的（受控）还是异常的（意外）。

代码	字段	问题描述
RSLT	正常关机	关闭的性质： SUCS：系统已正常关闭。 DSDN：系统未完全关闭。 VRGN：系统在服务器安装（或重新安装）后首次启动。

该消息不指示主机服务器是否已启动，仅指示报告服务。此消息可用于：

- 检测审计跟踪中的不连续性。
- 确定服务在运行期间是否发生故障（因为 StorageGRID 系统的分布式特性可能会掩盖这些故障）。Server Manager 会自动重启发生故障的服务。