



查看审核日志 StorageGRID 11.5

NetApp
April 11, 2024

目录

查看审核日志	1
审核消息概述	1
审核日志文件和消息格式	7
审核消息和对象生命周期	25
审核消息	31

查看审核日志

了解StorageGRID 系统审核日志并查看所有审核消息的列表。

- ["审核消息概述"](#)
- ["审核日志文件和消息格式"](#)
- ["审核消息和对象生命周期"](#)
- ["审核消息"](#)

审核消息概述

这些说明包含有关 StorageGRID 审核消息和审核日志的结构和内容的信息。您可以使用此信息读取和分析系统活动的审核跟踪。

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 系统的审核消息。

我们假定您已对StorageGRID 系统中已审核活动的性质有了充分的了解。要使用文本日志文件，您必须有权访问管理节点上配置的审核共享。

相关信息

["管理 StorageGRID"](#)

审核消息流和保留

所有 StorageGRID 服务都会在系统正常运行期间生成审核消息。您应了解这些审核消息如何在StorageGRID 系统中移动到 `audit.log` 文件

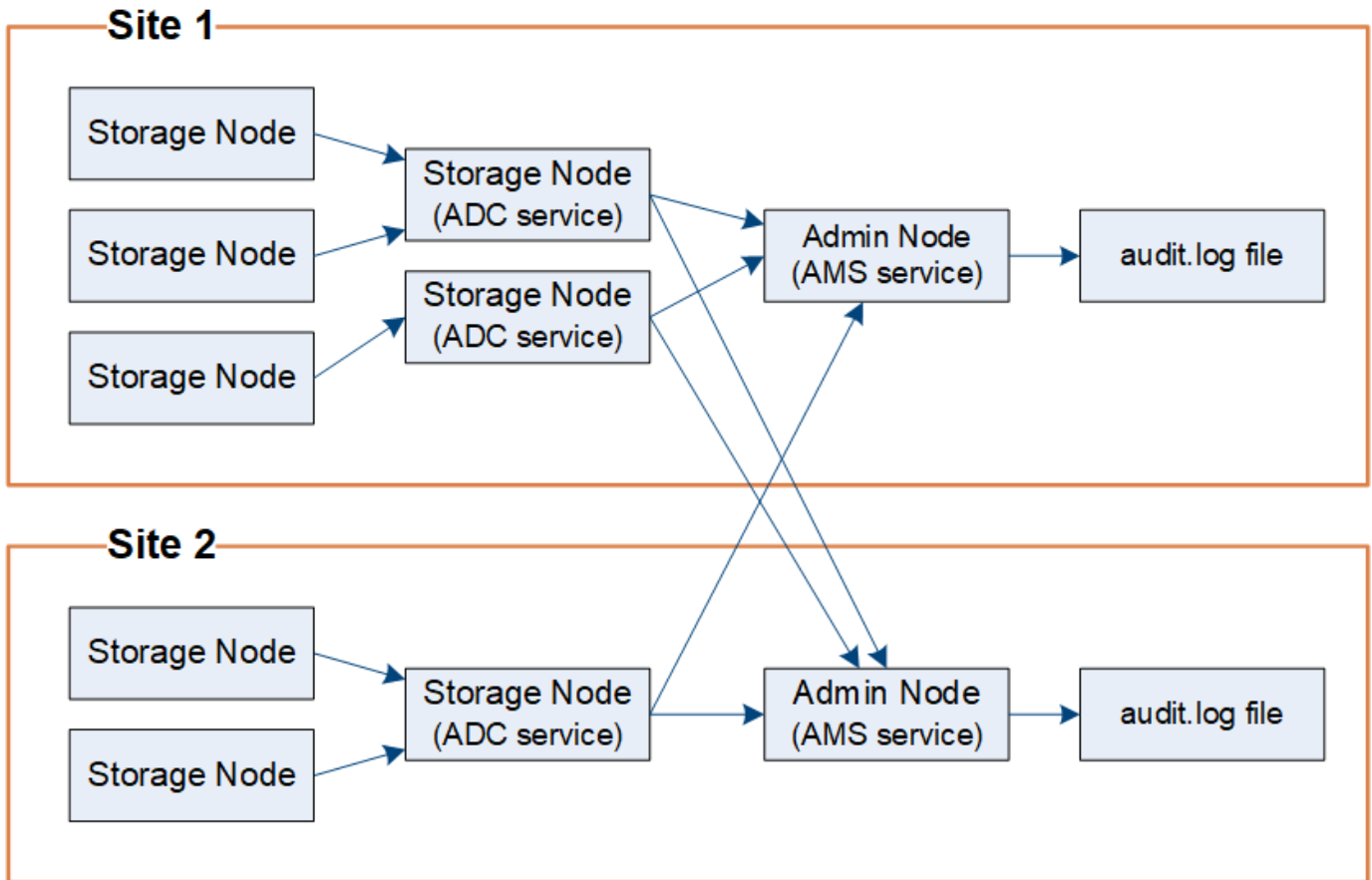
审核消息流

审核消息由管理节点以及具有管理域控制器（ADO）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一个模板服务。每个站点上安装的前三个存储节点会自动启用此 ADC-Service。

反过来，每个 ADC 服务都充当中继，并将其审核消息集合发送到 StorageGRID 系统中的每个管理节点，从而为每个管理节点提供完整的系统活动记录。

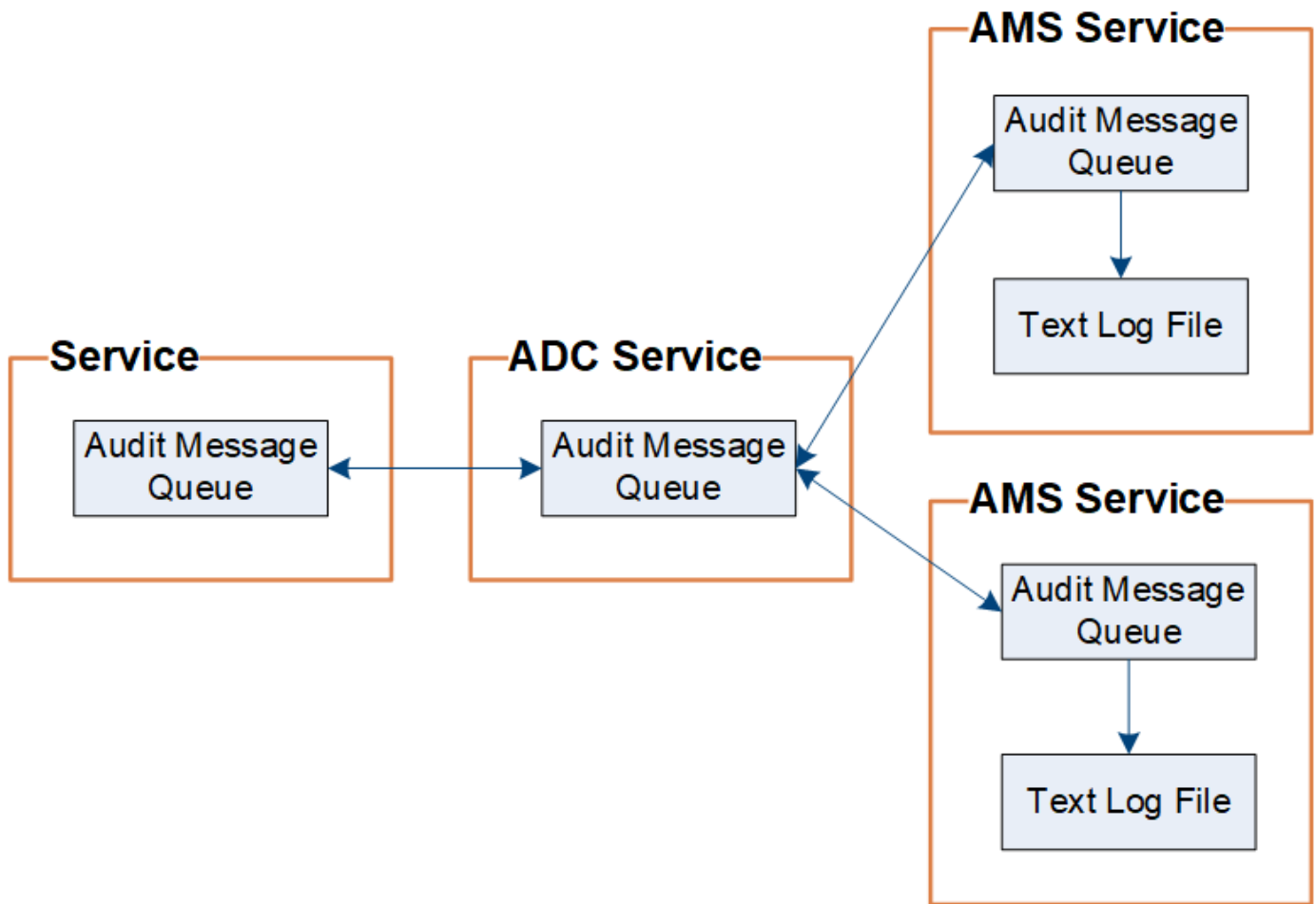
每个管理节点都会将审核消息存储在文本日志文件中；活动日志文件名为 `audit.log`。



审核消息保留

StorageGRID 使用复制和删除过程来确保在将审核消息写入审核日志之前不会丢失任何审核消息。

当节点生成或转发审核消息时，此消息会存储在网格节点的系统磁盘上的审核消息队列中。消息的副本始终保留在审核消息队列中、直到消息写入管理节点的审核日志文件为止 `/var/local/audit/export` 目录。这有助于防止传输期间丢失审核消息。



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中更多的可用空间 `/var/local/` 目录。如果问题描述 仍然存在，并且节点的审核消息目录过满，则各个节点将优先处理其积压工作，并暂时不可用于处理新消息。

具体来说，您可能会看到以下行为：

- 如果 `/var/local/audit/export` 管理节点使用的目录已满、管理节点将标记为不可用于新审核消息、直到目录不再全满为止。S3 和 Swift 客户端请求不受影响。如果无法访问审核存储库，则会触发 XAMS（无法访问审核存储库）警报。
- 如果 `/var/local/` 具有此ADA服务的存储节点使用的目录已满92%、此节点将被标记为不可用于审核消息、直到目录已满87%为止。对其他节点的 S3 和 Swift 客户端请求不受影响。如果无法访问审核中继，则会触发 NRLY（可用审核中继）警报。



如果没有可用于此ADA服务的存储节点、则存储节点会将审核消息存储在本地。

- 如果 `/var/local/` 存储节点使用的目录已满85%、此节点将开始拒绝S3和Swift客户端请求 503 Service Unavailable。

以下类型的问题可能会使发生原因 审核消息队列变得非常庞大：

- 管理节点或存储节点使用 ADC-Service 中断的情况。如果系统的一个节点已关闭，则其余节点可能会回记录。
- 超过系统审核容量的持续活动率。

- `/var/local/` 由于与审核消息无关的原因、一个模块存储节点上的空间已满。发生这种情况时，节点将停止接受新的审核消息，并优先处理当前的积压工作，而这可能会使发生原因回退到其他节点上。

大型审核队列警报和审核消息已排队（**Audit Messages Queued**，**AMQS**）警报

为了帮助您监控一段时间内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，将触发 * 大型审核队列 * 警报和原有 AMQS 警报。

如果触发了 * 大型审核队列 * 警报或原有 AMQS 警报，请首先检查系统上的负载—如果最近发生了大量事务，则警报和警报应随着时间的推移而解决，并且可以忽略。

如果警报或警报持续存在且严重性增加，请查看队列大小图表。如果此数量在数小时或数天内稳定增加，则审核负载可能已超过系统的审核容量。通过将客户端写入和客户端读取的审核级别更改为 " 错误 " 或 " 关闭 " 来降低客户端操作速率或减少记录的审核消息数量。请参见 "[更改审核消息级别](#)"。

重复的消息

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

更改审核消息级别

您可以调整审核级别、以增加或减少每个审核消息类别的审核日志中记录的审核消息数量。

您需要的内容

- 您必须使用支持的浏览器登录到网格管理器。
- 您必须具有特定的访问权限。

关于此任务

审核日志中记录的审核消息将根据*配置*>*监控*>*审核*页面上的设置进行筛选。

您可以为以下每种消息设置不同的审核级别：

- 系统：默认情况下、此级别设置为正常。
- 存储：默认情况下、此级别设置为错误。
- 管理：默认情况下、此级别设置为正常。
- 客户端读取：默认情况下、此级别设置为正常。
- 客户端写入：默认情况下、此级别设置为正常。



如果您最初使用 10.3 或更高版本安装 StorageGRID，则这些默认设置适用。如果您已从早期版本的 StorageGRID 升级，则所有类别的默认值均设置为正常。



升级期间，审核级别配置不会立即生效。

步骤

1. 选择*配置*>*监控*>*审核*。

Audit

Audit Levels

System	Normal
Storage	Error
Management	Normal
Client Reads	Normal
Client Writes	Normal

Audit Protocol Headers

Header Name 1	X-Forwarded-For	✕
Header Name 2	x-amz-*	+ ✕

Save

- 对于每个审核消息类别，从下拉列表中选择一个审核级别：

审核级别	Description
关闭	不会记录此类别中的任何审核消息。
error	仅会记录错误消息—审核结果代码不是 " 成功 " (SUC) 的消息。
正常	系统会记录标准事务处理消息，即这些说明中针对此类别列出的消息。
调试	已弃用。此级别的行为与正常审核级别相同。

对于任何特定级别，包含的消息都包括那些将在较高级别记录的消息。例如，正常级别包括所有错误消息。

- 在*审核协议标头*下，输入要包含在客户端读取和客户端写入审核消息中的HTTP请求标头的名称。使用星号(*)作为通配符、或者使用转义序列(*)作为文字星号。单击加号可创建标题名称字段列表。



审核协议标头仅适用于 S3 和 Swift 请求。

如果在请求中发现此类HTTP标头、则这些标头将包含在审核消息的HTRH字段下。



只有当 * 客户端读取 * 或 * 客户端写入 * 的审核级别不是 * 关闭 * 时，才会记录审核协议请求标头。

4. 单击 * 保存 *。

相关信息

["系统审核消息"](#)

["对象存储审核消息"](#)

["管理审核消息"](#)

["客户端读取审核消息"](#)

["管理 StorageGRID"](#)

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。为了便于访问审核日志、您可以配置客户端对NFS和CIFS (已弃用)的审核共享的访问权限。您也可以直接从管理节点的命令行访问审核日志文件。

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. 输入中列出的密码 `Passwords.txt` 文件

2. 转到包含审核日志文件的目录：

```
cd /var/local/audit/export
```

3. 根据需要查看当前审核日志文件或已保存的审核日志文件。

相关信息

["管理 StorageGRID"](#)

审核日志文件轮换

审核日志文件会保存到管理节点的中 `/var/local/audit/export` 目录。活动审核日志文件名为 `audit.log`。

每天执行一次活动 `audit.log` 此时将保存文件、并显示一个新的 `audit.log` 文件已启动。已保存文件的名称

以格式指示其保存的时间 `yyyy-mm-dd.txt`。如果在一天内创建了多个审核日志、则文件名将使用保存文件的日期、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` 是在2018年4月15日创建并保存的第一个和第二个日志文件。

一天之后、保存的文件将按格式进行压缩和重命名 `yyyy-mm-dd.txt.gz`、用于保留原始日期。随着时间的推移，这会导致为管理节点上的审核日志分配的存储被占用。脚本可监控审核日志空间占用情况、并根据需要删除日志文件以释放中的空间 `/var/local/audit/export` 目录。审核日志会根据创建日期进行删除，最早的日志会先删除。您可以在以下文件中监控脚本的操作：`/var/local/log/manage-audit.log`。

此示例显示了活动的 `audit.log` file、前一天的文件 (`2018-04-15.txt`)、以及前一天的压缩文件 (`2018-04-14.txt.gz`)。

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

审核日志文件和消息格式

您可以使用审核日志收集有关系统的信息并对问题进行故障排除。您应了解审核日志文件的格式以及审核消息使用的常规格式。

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.UUUUUU`、其中 `UUUUUU` 为微秒。

- 审核消息本身、括在方括号内、以开头 `AUDT`。

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::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]]
```

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` 用于获取审核日志中审核消息的简化摘要的工具。您可以使用 `audit-sum` 用于汇总记录了多少个写入、读取和删除操作以及这些操作所需的时间的工具。

相关信息

["使用audit-explain工具"](#)

["使用audit-sum工具"](#)

使用audit-explain工具

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

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

- `audit-explain` 主管理节点上提供的工具可在审核日志中提供审核消息的简化摘要。



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

此示例显示了中的典型输出 `audit-explain` 工具。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` 工具可以处理纯审核日志或压缩的审核日志。例如：

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

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

- `audit-explain` 该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、这样您可以使用筛选和预处理输入 `grep` 命令或其他方式。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和运行的部分来节省时间 `audit-explain` 而不是整个文件。



。 `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、请以命令行参数形式提供其文件名、或者使用 `zcat` 用于先解压缩文件的工具。例如：

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

使用 `help (-h)` 选项以查看可用选项。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. 输入中列出的密码 `Passwords.txt` 文件

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` 该工具可打印指定文件中所有消息的可读解释。



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、请使用时间戳 `(-t)` 选项。

相关信息

["SPUT : S3 PUT"](#)

使用 `audit-sum` 工具

您可以使用 `audit-sum` 用于计算写入、读取、磁头和删除审核消息的计数以及查看每种操作类型的最小、最大和平均时间(或大小)的工具。

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

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



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

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

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			

。 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` 该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、这样您可以使用筛选和预处理输入 `grep` 命令或其他方式。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、请以命令行参数形式提供其文件名、或者使用 `zcat` 用于先解压缩文件的工具。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、摘要显示最小、最大和平均操作时间、但您可以使用 `size (-s)` 可选择查看对象大小。

使用 `help (-h)` 选项以查看可用选项。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. 输入中列出的密码 `Passwords.txt` 文件
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
```

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

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消息并添加长输出选项 (-l)以包括对象路径：`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/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

```

+ 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. 如果要确定要在网格中输入和检索的对象大小、请使用size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使用问题描述 命令并使用group-by-time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、请添加size选项 (-s)到命令:

```
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` 用于查看该小时内所有SGET操作的工具：

```
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、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、用于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、用于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.ltd002	1564563	0.011	51.569
0.361			

- c. 要确定哪些分段的SPUT对象大小最大、请使用这两个 `-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

相关信息

["使用audit-explain工具"](#)

审核消息格式

在 StorageGRID 系统中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。

如果提供的摘要信息 `audit-explain` 和 `audit-sum` 工具不足、请参见本节以了解所有审核消息的常规格式。

下面是可能显示在审核日志文件中的审核消息示例：

```
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。整个字符串用方括号括起来 ([])、并且字符串中的每个属性元素都具有以下特征：

- 括在方括号中 []
- 由字符串引入 AUDT、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

每个元素都包含一个属性代码，一个数据类型以及一个以以下格式报告的值：

```
[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。

以下列表介绍了这些属性元素：

- ATTR 是所报告属性的四字符代码。某些属性对于所有审核消息都是通用的，而其他属性则针对事件。
- type 是值的编程数据类型的四字符标识符、例如UI64、FC32等。此类型用圆括号括起来 ()。
- value 是属性的内容、通常为数字或文本值。值始终后跟一个冒号 (:)。数据类型CStr的值被双引号括起来 " "。

相关信息

["使用audit-explain工具"](#)

["使用audit-sum工具"](#)

["审核消息"](#)

["审核消息中的常见元素"](#)

["数据类型"](#)

["审核消息示例"](#)

数据类型

使用不同的数据类型将信息存储在审核消息中。

Type	Description
UI32	无符号长整数（32位）；它可以存储0到4,294,967,295之间的数字。
UI64	无符号双长整数（64位）；它可以存储0到18,446,744,073,709,551,615之间的数字。
FC32	四字符常量；一个32位无符号整数值，表示为四个ASCII字符，如"ABCD"。
iPad	用于IP地址。

Type	Description
CStr	<p>一个长度可变的数组，由 UTF-8 - 字符组成。可以按照以下约定对字符进行转义：</p> <ul style="list-style-type: none"> • 反斜杠为 \。 • 回车符为 • 双引号为 "。 • 换行符（新行）为 • 字符可以替换为其十六进制等效项（格式为 \xHH，其中 HH 是表示该字符的十六进制值）。

事件专用数据

审核日志中的每个审核消息都会记录特定于系统事件的数据。

在会议开始后 [AUDT: 用于标识消息本身的容器、下一组属性提供有关审核消息所述事件或操作的信息。以下示例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) : "60025621595611246499"] [SACC (CSTR) : "account"]
[S3AK (CSTR) : "SGKH4_Nc8S01H6w3w0nCOFCGgk__E6dYzKlumRsKJA=="]
[SUSR (CSTR) : "urn:sgws:identity::60025621595611246499:root"]
[SBAI (CSTR) : "60025621595611246499"] [SBAC (CSTR) : "account"] [S3BK (CSTR) : "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] [AMID (FC32) : S3RQ] [ATID (UI64) : 15552417629170647261]]
```

。ATYP Element (在示例中带有下划线)用于标识生成消息的事件。此示例消息包含 Shea 消息代码 ([ATYP (FC32) : Shea])，表示此消息是由成功的 S3 head 请求生成的。

相关信息

["审核消息中的常见元素"](#)

["审核消息"](#)

审核消息中的常见元素

所有审核消息都包含通用要素。

代码	Type	Description
在中	FC32	模块 ID：生成消息的模块 ID 的四个 - 字符标识符。这表示生成审核消息的代码段。

代码	Type	Description
ANID	UI32	Node 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，系统会为每个服务分配一个唯一的标识符。无法更改此 ID。
ASE	UI64	审核会话标识符：在先前版本中，此元素表示在服务启动后初始化审核系统的时间。此时间值是自操作系统 Epoch（1970 年 1 月 1 日 00：00：00 UTC）以来以微秒为单位测量的。 • 注：* 此元素已废弃，不再显示在审核消息中。
ASQN	UI64	序列计数：在先前版本中，对于网格节点（ANID）上生成的每个审核消息，此计数器会递增，并在服务重新启动时重置为零。 • 注：* 此元素已废弃，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。
Atim	UI64	timestamp：生成触发审核消息的事件的时间，以操作系统 Epoch（1970 年 1 月 1 日 00：00：00 UTC）之后的微秒为单位。请注意，用于将时间戳转换为本地日期和时间的大多数可用工具均以毫秒为基础。 可能需要对记录的时间戳进行舍入或截断。在中审核消息开头显示的人员 - 可读时间 audit.log file 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 是一个文字字符串、用于指示日期时间段的开始。UUUUUU 为微秒。
ATYP	FC32	Event Type：所记录事件的四 - 字符标识符。这将控制消息的 "有效负载" 内容：包含的属性。
保护程序	UI32	version：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核报告中加入新功能。通过此字段，可以在 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	result：事件，进程或事务的结果。如果与消息无关，则不会使用 none 而不是 SUC，这样就不会意外筛选该消息。

审核消息示例

您可以在每个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。

下面是可能显示在中的示例审核消息 audit.log 文件：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"]
[S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][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]]
```

审核消息包含有关所记录事件的信息以及有关审核消息本身的信息。

要确定审核消息记录的事件，请查找 ATYP 属性（突出显示在下方）：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"]
[S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][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，用于记录对象载入到存储分段的情况。

以下审核消息还会显示与对象关联的存储分段：

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"]
[S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][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 事件发生的时间，请注意审核消息开头的通用协调时间（UTC）时间戳。此值为审核消息本身的 ATIM 属性的用户 - 可读版本：

2014-07-17T21:17:58.959669

```
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][S3KY(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):1579224144102530435]]
```

Atim 会以微秒为单位记录自 UNIX Epoch 开始以来的时间。在示例中、为值 1405631878959669 转换为2014年7月17日星期四21: 17: 59 UTC。

相关信息

["SPUT : S3 PUT"](#)

["审核消息中的常见元素"](#)

审核消息和对象生命周期

每次载入，检索或删除对象时都会生成审核消息。您可以通过查找特定于 API（S3 或 Swift）的审核消息在审核日志中标识这些事务。

审核消息通过每个协议专用的标识符进行链接。

协议	代码
链接 S3 操作	S3BK（S3 分段）和 / 或 S3KY（S3 密钥）
链接 Swift 操作	WCON（Swift 容器）和 / 或 WOBJ（Swift 对象）
链接内部操作	CBID（对象的内部标识符）

审核消息的时间

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。

信息生命周期管理策略配置

使用默认 ILM 策略（基线 2 副本），对象数据复制一次，总共复制两个副本。如果 ILM 策略需要两个以上的副本，则每个额外的副本还会另外显示一组 CBRE，CBSE 和 SCMT 消息。有关 ILM 策略的详细信息，请参见有关通过信息生命周期管理管理对象的信息。

归档节点

归档节点向外部归档存储系统发送对象数据时生成的一系列审核消息与存储节点的类似，只是没有 SCMT（存储对象提交）消息。对于对象数据的每个归档副本，系统会生成 ATCE（Archive Object Store Begin）和 ASCE（Archive Object Store End）消息。

归档节点从外部归档存储系统检索对象数据时生成的一系列审核消息与存储节点的类似，只是为每个检索到的对象数据副本生成了 ARCB（归档对象检索开始）和 Arce（归档对象检索结束）消息。

归档节点从外部归档存储系统删除对象数据时生成的一系列审核消息与存储节点的类似，只是没有 Srem（对象存储删除）消息，并且每个删除请求都有一条 AREM（归档对象删除）消息。

相关信息

["使用 ILM 管理对象"](#)

对象载入事务

您可以通过查找特定于 API（S3 或 Swift）的审核消息，在审核日志中确定客户端载入事务。

下表列出了在载入事务期间生成的并非所有审核消息。仅包含跟踪载入事务所需的消息。

S3 载入审核消息

代码	Name	Description	跟踪	请参见
SPUT	S3 PUT 事务	S3 PUT 载入事务已成功完成。	CBID， S3BK， S3KY	"SPUT： S3 PUT"
ORLM	符合对象规则	已对此对象满足 ILM 策略要求。	CBID	"ORLM：符合对象规则"

Swift 载入审核消息

代码	Name	Description	跟踪	请参见
WWPUT	Swift PUT 事务	Swift PUT 载入事务已成功完成。	CBID， WCON， WOBJ	"WWPUT： Swift PUT"
ORLM	符合对象规则	已对此对象满足 ILM 策略要求。	CBID	"ORLM：符合对象规则"

示例：**S3** 对象载入

下面的一系列审核消息是在 S3 客户端将对象载入存储节点（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 策略包括常用 ILM 规则，创建 2 个副本。



在以下示例中并未列出事务期间生成的所有审核消息。仅列出与 S3 载入事务（SPUT）相关的那些。

此示例假设先前已创建 S3 存储分段。

SPUT : S3 PUT

此时将生成 SPUT 消息，以指示已发出 S3 PUT 事务，以便在特定存储分段中创建对象。

```
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"]<strong
class="S3KY(CSTR):"testobject-0-
3"">[CBID(UI64):0x8EF52DF8025E63A8]</strong>[CSIZ(UI64):30720][AVER(UI32):
10]<strong
class="ATIM(UI64):150032627859669">[ATYP(FC32):SPUT]</strong>[ANID(UI32):1
2086324][AMID(FC32):S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM : 符合对象规则

ORLM 消息指示已对此对象满足 ILM 策略要求。此消息包含对象的 CBID 以及应用的 ILM 规则的名称。

对于复制的对象，"LOC" 字段包含对象位置的 LDR 节点 ID 和卷 ID。

```
2019-07-17T21:18:31.230669[AUDT:
<strong>[CBID(UI64):0x50C4F7AC2BC8EDF7]</strong> [RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"]<strong class="LOCS(CSTR):*"CLDI 12828634
2148730112">[RSLT(FC32):SUCS][AVER(UI32):10] [ATYP(FC32):ORLM]</strong>
[ATIM(UI64):1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):131
00453][AMID(FC32):BCMS]]
```

对于经过纠删编码的对象，LOC 字段包括纠删编码配置文件 ID 和纠删编码组 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][ATYP(FC32):ORLM][ANID(UI32):12355278][AMI
D(FC32):ILMX][ATID(UI64):4168559046473725560]]
```

路径字段包括 S3 存储分段和密钥信息或 Swift 容器和对象信息，具体取决于所使用的 API。

```
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]]
```

对象删除事务

您可以通过查找特定于 API（S3 和 Swift）的审核消息来确定审核日志中的对象删除事务。

下表列出了在删除事务期间生成的并非所有审核消息。仅包含跟踪删除事务所需的消息。

S3 删除审核消息

代码	Name	Description	跟踪	请参见
SDEL	S3 删除	请求从存储分段中删除对象。	CBID , S3KY	"SDEL : S3 delete"

Swift 删除审核消息

代码	Name	Description	跟踪	请参见
WDEL	Swift 删除	请求从容器或容器中删除对象。	CBID , WOBJ	"WDEL : Swift 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，系统会生成一条审核消息并将其保存到审核日志中。



在删除事务期间生成的审核消息并非都在以下示例中列出。仅列出与 S3 删除事务（SDEL）相关的那些。

SDEL : S3 删除

当客户端向 LDR 服务发送删除对象请求时，对象删除即开始。此消息包含用于删除对象的存储分段以及用于标识对象的 S3 密钥。

```

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"] <strong>[S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
7"] [CBID(UI64):0x339F21C5A6964D89]</strong>
[CSIZ(UI64):30720][AVER(UI32):10][ATIM(UI64):150032627859669]
<strong>[ATYP(FC32):SDEL]</strong>[ANID(UI32):12086324][AMID(FC32):S3RQ][A
TID(UI64):4727861330952970593]]

```

对象检索事务

您可以通过查找特定于 API（S3 和 Swift）的审核消息来确定审核日志中的对象检索事务。

下表列出了在检索事务期间生成的并非所有审核消息。仅包含跟踪检索事务所需的消息。

S3 检索审核消息

代码	Name	Description	跟踪	请参见
SGET	S3 GET	请求从存储分段中检索对象。	CBID , S3BK , S3KY	"SGET : S3 GET"

Swift 检索审核消息

代码	Name	Description	跟踪	请参见
wget	Swift GET	请求从容器中检索对象。	CBID , WCON , WOBJ	"WGET : Swift 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，系统会生成一条审核消息并将其保存到审核日志中。

请注意，并非在事务期间生成的所有审核消息都在以下示例中列出。仅列出与 S3 检索事务（SGET）相关的那些。

SGET : S3 GET

当客户端向 LDR 服务发送获取对象请求时，对象检索即开始。此消息包含用于检索对象的存储分段以及用于标识对象的 S3 密钥。

```

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][CSIZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605][ATYP(FC32):SGET][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]]

```

如果存储分段策略允许，客户端可以匿名检索对象，或者从其他租户帐户拥有的存储分段中检索对象。审核消息包含有关存储分段所有者的租户帐户的信息，以便您可以跟踪这些匿名请求和跨帐户请求。

在以下示例消息中，客户端会为存储在非自有存储分段中的对象发送 GET 对象请求。SBAI 和 SBAC 的值会记录存储分段所有者的租户帐户 ID 和名称，这与 S3AI 和 SACC 中记录的租户帐户 ID 和客户端名称不同。

```

2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]
<strong>[S3AI(CSTR):"17915054115450519830"][SACC(CSTR):"s3-account-b"]</strong>[S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="<strong
rong
class="SUSR(CSTR):"urn:sgws:identity::17915054115450519830:root"">[SBAI(CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-a"]</strong>[S3BK(CSTR):"bucket-anonymou
s"] [S3KY(CSTR):"Hello.txt"] [CBID(UI64):0x83D70C6F1F662B02] [CSIZ(UI64):12] [AVER(UI32):10] [ATIM(UI64):1505947995876415] [ATYP(FC32):SGET] [ANID(UI32):12272050] [AMID(FC32):S3RQ] [ATID(UI64):6888780247515624902]]

```

元数据更新消息

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	Name	Description	跟踪	请参见
SUPD	已更新 S3 元数据	当 S3 客户端更新已载入对象的元数据时生成。	CBID , S3KY , HTRH	"SUPD : 已更新 S3 元数据"

示例：S3 元数据更新

此示例显示了更新现有 S3 对象的元数据的成功事务。

SUPD : S3 元数据更新

S3客户端请求(SUPD)更新指定的元数据(x-amz-meta-)。在此示例中、请求标头包含在字段HTRH中、因为它已配置为审核协议标头("配置">"监控">"审核")。

```
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]]
```

相关信息

["更改审核消息级别"](#)

审核消息

以下各节列出了系统返回的审核消息的详细说明。每个审核消息首先列在一个表中，该表按相关消息所代表的活动类别对相关消息进行分组。这些分组对于了解要审核的活动类型以及选择所需的审核消息筛选类型都很有用。

审核消息也会按其四个字符的代码的字母顺序列出。此字母列表可用于查找有关特定消息的信息。

本章中使用的四字符代码是审核消息中的 ATYP 值，如以下示例消息所示：

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][<stro
ng>ATYP(FC32):SYSU</strong>][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(
UI64):9445736326500603516]]
```

相关信息

"审核消息"

"更改审核消息级别"

审核消息类别

您应熟悉对审核消息进行分组的各个类别。这些组将根据消息表示的活动类别进行组织。

系统审核消息

您应熟悉属于系统审核类别的审核消息。这些事件与审核系统本身，网格节点状态，系统范围的任务活动（网格任务）和服务备份操作相关，可帮助您解决潜在问题。

代码	消息标题和问题描述	请参见
ECOC	Erase 编码数据片段损坏：表示检测到擦除编码数据片段损坏。	"EcC：擦除编码数据片段损坏"
ETAF	安全身份验证失败：尝试使用传输层安全（Transport Layer Security，TLS）进行连接失败。	"ETAF：安全身份验证失败"
GNRG	GNDS 注册：服务在 StorageGRID 系统中更新或注册了有关自身的信息。	"GNRG：GNDS 注册"
GNUR	GNDS 注销：服务已从 StorageGRID 系统中注销自身。	"GN-R：GNDS 注销"
GTED	网格任务已结束：CMN 服务已完成网格任务的处理。	"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。	"GTST：已启动网格任务"
GTSU	已提交网格任务：已将网格任务提交到 CMN 服务。	"GTSU：已提交网格任务"
标识	ILM Initiated Delete：当 ILM 开始删除对象的过程时，会生成此审核消息。	"idel：ILM 已启动删除"
LKCU	已覆盖对象清理。自动删除已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"

代码	消息标题和问题描述	请参见
LLST	Location Lost：当某个位置丢失时，会生成此审核消息。	"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"
ORLM	满足对象规则：对象数据按照 ILM 规则的指定进行存储。	"ORLM：符合对象规则"
Sadd	禁用安全审核：已关闭审核消息日志记录。	"Sadd：禁用安全审核"
Sade	启用安全审核：审核消息日志记录已还原。	"Sade：启用安全审核"
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"
系统	节点停止：已请求关闭。	"SYSD：节点停止"
系统	节点停止：服务已正常停止。	"Syst：节点正在停止"
系统	节点启动：服务已启动；消息中显示了上次关闭的性质。	"SYSU：节点启动"
VLST	用户启动的卷丢失： /proc/CMSI/Volume_Lost 命令已运行。	"VLST：用户启动的卷丢失"

相关信息

"LKCU：覆盖对象清理"

对象存储审核消息

您应熟悉属于对象存储审核类别的审核消息。这些事件与 StorageGRID 系统中对象的存储和管理相关。其中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。

代码	Description	请参见
APCT	从云层清除归档：已归档的对象数据将从外部归档存储系统中删除，该系统通过 S3 API 连接到 StorageGRID 。	"APCT：从云层清除归档"
ARCB	归档对象检索开始：ARC-Service 开始从外部归档存储系统检索对象数据。	"ARCB：开始归档对象检索"
Arce	归档对象检索结束：对象数据已从外部归档存储系统中检索，并且 ARC-Service 会报告检索操作的状态。	"Arce：归档对象检索结束"
ARCT	从云层检索归档：归档对象数据从外部归档存储系统中检索，该系统通过 S3 API 连接到 StorageGRID 。	"ARCT：从云层检索归档"
AREM	归档对象删除：已从外部归档存储系统成功或未成功删除内容块。	"AREM：归档对象删除"
ASCE	归档对象存储结束：已将内容块写入外部归档存储系统，并且 ARC-Service 会报告写入操作的状态。	"ASCE：归档对象存储结束"
上一个月	归档存储云层：对象数据存储到外部归档存储系统，该系统通过 S3 API 连接到 StorageGRID 。	"SCT：归档存储云层"
ATCE	归档对象存储开始：已开始向外部归档存储写入内容块。	"ATCE：开始归档对象存储"
AVCC	归档验证云层配置：提供的帐户和存储分段设置已成功验证或未成功验证。	"AVCC：归档验证云层配置"
CBSE	对象发送结束：源实体完成了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：对象接收结束"
SCMT	对象存储提交：内容块已完全存储和验证，现在可以请求。	"SCMT：对象存储提交"

代码	Description	请参见
Srem	对象存储删除：已从网格节点中删除内容块，无法再直接请求。	"Srem：对象存储删除"

客户端读取审核消息

当 S3 或 Swift 客户端应用程序请求检索对象时，系统会记录客户端读取审核消息。

代码	Description	使用人	请参见
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。 • 注：* 如果事务对子资源执行操作，则审核消息将包含字段 S3SR。 。	S3 客户端	"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。	S3 客户端	"Shea：S3 机头"
wget	Swift get：记录成功的事务以检索对象或列出容器中的对象。	Swift 客户端	"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。	Swift 客户端	"WHEA：Swift head"

客户端写入审核消息

当 S3 或 Swift 客户端应用程序请求创建或修改对象时，系统会记录客户端写入审核消息。

代码	Description	使用人	请参见
OVWR	对象覆盖：记录一个事务，以便使用另一个对象覆盖一个对象。	S3 客户端 Swift 客户端	"OVWR：对象覆盖"

代码	Description	使用人	请参见
SDEL	S3 delete：记录成功的事务以删除对象或存储分段。 • 注：* 如果事务对子资源执行操作，则审核消息将包含字段 S3SR。	S3 客户端	"SDEL：S3 delete"
SPOS	S3 POST：记录将对象从 AWS Glacier 存储还原到云存储池的成功事务。	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分段。 • 注：* 如果事务对子资源执行操作，则审核消息将包含字段 S3SR。	S3 客户端	"SPUT：S3 PUT"
SUPD	S3 元数据已更新：记录成功的事务以更新现有对象或存储分段的元数据。	S3 客户端	"SUPD：已更新 S3 元数据"
WDEL	Swift delete：记录成功的事务以删除对象或容器。	Swift 客户端	"WDEL：Swift delete"
WWPUT	Swift PUT：记录成功的事务以创建新对象或容器。	Swift 客户端	"WWPUT：Swift PUT"

管理审核消息

"管理" 类别可将用户请求记录到管理 API。

代码	消息标题和问题描述	请参见
MGAU	Management API 审核消息：用户请求日志。	"MGAU：管理审核消息"

审核消息

发生系统事件时、StorageGRID 系统会生成审核消息并将其记录在审核日志中。

APCT：从云层清除归档

从通过 S3 API 连接到 StorageGRID 的外部归档存储系统中删除归档对象数据时会生成此消息。

代码	字段	Description
CBID	内容块 ID	已删除的内容块的唯一标识符。
CSIZ	内容大小	对象的大小（以字节为单位）。始终返回 0。
RSLT	结果代码	返回成功（SUC）或后端报告的错误。
SUID	存储唯一标识符	从中删除对象的云层的唯一标识符（UUID）。

ARCB：开始归档对象检索

在请求检索归档的对象数据且检索过程开始时生成此消息。检索请求会立即处理，但可以重新排序，以提高从磁带等线性介质检索的效率。

代码	字段	Description
CBID	内容块 ID	要从外部归档存储系统检索的内容块的唯一标识符。
RSLT	结果	指示启动归档检索过程的结果。当前定义的值为：suC：已收到内容请求并排队等待检索。

此审核消息用于标记归档检索的时间。通过该选项，您可以将该消息与相应的 Arce End 消息进行匹配，以确定归档检索的持续时间以及操作是否成功。

Arce：归档对象检索结束

当归档节点尝试从外部归档存储系统检索对象数据时，将生成此消息。如果成功，则此消息指示已从归档位置完全读取请求的对象数据，并已成功验证。检索并验证对象数据后，这些数据将传送到请求服务。

代码	字段	Description
CBID	内容块 ID	要从外部归档存储系统检索的内容块的唯一标识符。

代码	字段	Description
VLID	卷标识符	归档数据的卷的标识符。如果未找到内容的归档位置，则返回卷 ID 0。
RSLT	检索结果	归档检索过程的完成状态： <ul style="list-style-type: none"> • SUC：成功 • VRFL：失败（对象验证失败） • Arun：失败（外部归档存储系统不可用） • 取消：失败（已取消检索操作） • GERR：失败（一般错误）

将此消息与相应的 ARCB 消息进行匹配可以指示执行归档检索所需的时间。此消息指示检索是否成功，如果失败，则指示检索内容块失败的发生原因。

ARCT：从云层检索归档

从通过 S3 API 连接到 StorageGRID 的外部归档存储系统检索归档对象数据时会生成此消息。

代码	字段	Description
CBID	内容块 ID	已检索到的内容块的唯一标识符。
CSIZ	内容大小	对象的大小（以字节为单位）。此值仅适用于成功检索。
RSLT	结果代码	返回成功（SUC）或后端报告的错误。
SUID	存储唯一标识符	外部归档存储系统的唯一标识符（UUID）。
时间	时间	请求的总处理时间，以微秒为单位。

AREM：归档对象删除

" 归档对象删除 " 审核消息指示已从归档节点成功删除内容块或未成功删除内容块。如果结果成功，则归档节点已成功通知外部归档存储系统 StorageGRID 已释放对象位置。对象是否从外部归档存储系统中删除取决于系统类型及其配置。

代码	字段	Description
CBID	内容块 ID	要从外部归档介质系统检索的内容块的唯一标识符。
VLID	卷标识符	用于归档对象数据的卷的标识符。
RSLT	结果	归档删除过程的完成状态： <ul style="list-style-type: none"> • SUC：成功 • Arun：失败（外部归档存储系统不可用） • GERR：失败（一般错误）

ASCE：归档对象存储结束

此消息表示向外部归档存储系统写入内容块的操作已结束。

代码	字段	Description
CBID	内容块标识符	存储在外部归档存储系统上的内容块的标识符。
VLID	卷标识符	将对象数据写入到的归档卷的唯一标识符。
VRN	已启用验证	指示是否对内容块执行验证。当前定义的值为： <ul style="list-style-type: none"> • vena：已启用验证 • VDSA：已禁用验证
MCLS	管理类	一个字符串，用于标识内容块分配到的 TSM 管理类（如果适用）。
RSLT	结果	指示归档过程的结果。当前定义的值为： <ul style="list-style-type: none"> • SUC：成功（归档过程成功） • OFFL：失败（归档已脱机） • VRFL：失败（对象验证失败） • Arun：失败（外部归档存储系统不可用） • GERR：失败（一般错误）

此审核消息表示指定的内容块已写入外部归档存储系统。如果写入失败，则结果将提供有关故障发生位置的基本故障排除信息。有关归档故障的更多详细信息，请参见 StorageGRID 系统中的归档节点属性。

SCT：归档存储云层

将归档对象数据存储到外部归档存储系统时会生成此消息，该系统通过 S3 API 连接到 StorageGRID。

代码	字段	Description
CBID	内容块 ID	已检索到的内容块的唯一标识符。
CSIZ	内容大小	对象的大小（以字节为单位）。
RSLT	结果代码	返回成功（SUC）或后端报告的错误。
SUID	存储唯一标识符	存储内容的云层的唯一标识符（UUID）。
时间	时间	请求的总处理时间，以微秒为单位。

ATCE：开始归档对象存储

此消息表示已开始向外部归档存储写入内容块。

代码	字段	Description
CBID	内容块 ID	要归档的内容块的唯一标识符。
VLID	卷标识符	将内容块写入到的卷的唯一标识符。如果操作失败，则返回卷 ID 0。

代码	字段	Description
RSLT	结果	指示内容块传输的结果。当前定义 的值为： <ul style="list-style-type: none"> • SUC：成功（已成功存储内容块） • exis：忽略（内容块已存储） • ISFD：发生故障（磁盘空间不足） • ster：失败（存储 CBID 时出错） • OFFL：失败（归档已脱机） • GERR：失败（一般错误）

AVCC：归档验证云层配置

验证 Cloud Tiering - Simple Storage Service（S3）目标类型的配置设置时，会生成此消息。

代码	字段	Description
RSLT	结果代码	返回成功（SUC）或后端报告的错误。
SUID	存储唯一标识符	与要验证的外部归档存储系统关联的 UUID。

CBRB：对象接收开始

在正常系统操作期间，随着数据的访问，复制和保留，内容块会在不同节点之间持续传输。在启动将内容块从一个节点传输到另一个节点时，目标实体会发出此消息。

代码	字段	Description
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	要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启动： <ul style="list-style-type: none"> push：发送实体请求传输操作。 Pull：接收实体请求传输操作。

代码	字段	Description
CTSR	源实体	CBID 传输的源（发送方）的节点 ID。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID。
CTSS	起始序列计数	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	指示上次请求的序列计数。如果传输成功，则在收到此序列计数后，此传输将视为已完成。
RSLT	传输开始状态	传输开始时的状态： SUCS：已成功启动传输。

此审核消息表示已对一个内容段启动节点到节点数据传输操作，该内容段通过其内容块标识符进行标识。该操作会从“开始序列计数”到“预期结束序列计数”请求数据。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，如果与存储审核消息结合使用，则用于验证副本计数。

CBRE：对象接收结束

内容块从一个节点传输到另一个节点完成后，此消息将由目标实体发出。

代码	字段	Description
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	要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启动： push：发送实体请求传输操作。 Pull：接收实体请求传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID。

代码	字段	Description
CTSS	起始序列计数	指示开始传输的顺序计数。
CTA	实际结束序列计数	指示上次成功传输的序列号。如果实际结束序列计数与开始序列计数相同，并且传输结果未成功，则不会交换任何数据。
RSLT	传输结果	<p>传输操作的结果（从发送实体的角度来看）：</p> <p>SUC：传输成功完成；已发送请求的所有序列计数。</p> <p>CONL：传输期间连接丢失</p> <p>CTMO：建立或传输期间连接超时</p> <p>UNDE：无法访问目标节点 ID</p> <p>CRPT：由于接收到损坏或无效的数据（可能表示发生篡改），传输已结束</p>

此审核消息表示节点到节点数据传输操作已完成。如果传输结果成功，则该操作会将数据从 " 开始序列计数 " 传输到 " 实际结束序列计数 "。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，以及查找错误，对错误进行制表和分析。与存储审核消息结合使用时，还可以用于验证副本计数。

CBSB：对象发送开始

在正常系统操作期间，随着数据的访问，复制和保留，内容块会在不同节点之间持续传输。在启动将内容块从一个节点传输到另一个节点时，源实体会发出此消息。

代码	字段	Description
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	要传输的内容块的唯一标识符。
CTDR	传输方向	<p>指示 CBID 传输是推送启动还是拉启动：</p> <p>push：发送实体请求传输操作。</p> <p>Pull：接收实体请求传输操作。</p>

代码	字段	Description
CTSR	源实体	CBID 传输的源（发送方）的节点 ID。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID。
CTSS	起始序列计数	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	指示上次请求的序列计数。如果传输成功，则在收到此序列计数后，此传输将视为已完成。
RSLT	传输开始状态	传输开始时的状态： SUCS：已成功启动传输。

此审核消息表示已对一个内容段启动节点到节点数据传输操作，该内容段通过其内容块标识符进行标识。该操作会从“开始序列计数”到“预期结束序列计数”请求数据。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，如果与存储审核消息结合使用，则用于验证副本计数。

CBSE：对象发送结束

在将内容块从一个节点传输到另一个节点后，源实体会发出此消息。

代码	字段	Description
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	要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启动： push：发送实体请求传输操作。 Pull：接收实体请求传输操作。
CTSR	源实体	CBID 传输的源（发送方）的节点 ID。
CTD	目标实体	CBID 传输的目标（接收器）的节点 ID。

代码	字段	Description
CTSS	起始序列计数	指示开始传输的顺序计数。
CTA	实际结束序列计数	指示上次成功传输的序列号。如果实际结束序列计数与开始序列计数相同，并且传输结果未成功，则不会交换任何数据。
RSLT	传输结果	<p>传输操作的结果（从发送实体的角度来看）：</p> <p>SUC：传输成功完成；已发送请求的所有序列计数。</p> <p>CONL：传输期间连接丢失</p> <p>CTMO：建立或传输期间连接超时</p> <p>UNDE：无法访问目标节点 ID</p> <p>CRPT：由于接收到损坏或无效的数据（可能表示发生篡改），传输已结束</p>

此审核消息表示节点到节点数据传输操作已完成。如果传输结果成功，则该操作会将数据从 "开始序列计数" 传输到 "实际结束序列计数"。发送和接收节点通过其节点 ID 进行标识。此信息可用于跟踪系统数据流，以及查找错误，对错误进行制表和分析。与存储审核消息结合使用时，还可以用于验证副本计数。

EcC：擦除编码数据片段损坏

此审核消息指示系统检测到经过纠删编码的数据片段已损坏。

代码	字段	Description
VCCO	VCS ID	包含损坏区块的 VCS 的名称。
VLID	卷 ID	包含损坏的纠删编码片段的 RangeDB 卷。
CCID	区块 ID	已损坏的纠删编码片段的标识符。
RSLT	结果	此字段的值为 "无"。RSLT- 是一个必填消息字段，但与此特定消息无关。使用 "无" 而不是 "CSU"，因此不会筛选此消息。

ETAf : 安全身份验证失败

如果尝试使用传输层安全（Transport Layer Security，TLS）进行连接失败，则会生成此消息。

代码	字段	Description
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。
RID	用户身份	表示远程用户身份的服务相关标识符。
RSLT	原因代码	失败的原因： SCNI：安全连接建立失败。 CERM：证书缺失。 证书：证书无效。 cere：证书已过期。 CERR：证书已撤销。 CSGN：证书签名无效。 CSGU：证书签名者未知。 UCRM：缺少用户凭据。 UCRI：用户凭据无效。 UCRU：不允许使用用户凭据。 tout：身份验证超时。

在与使用 TLS 的安全服务建立连接后，系统会使用 TLS 配置文件和服务中内置的其他逻辑来验证远程实体的凭据。如果此身份验证因证书或凭据无效，意外或不允许而失败，则会记录审核消息。这样可以查询未经授权的访问尝试以及其他与安全相关的连接问题。

此消息可能是由于远程实体的配置不正确或尝试向系统提供无效或不允许的凭据而导致的。应监控此审核消息，以检测未经授权访问系统的尝试。

GNRG : GNDS 注册

如果某个服务在 StorageGRID 系统中更新或注册了有关自身的信息，则 CMN 服务将生成此审核消息。

代码	字段	Description
RSLT	结果	更新请求的结果： <ul style="list-style-type: none"> • SUC：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。
GNTTP	设备类型	网格节点的设备类型（例如 LDR 服务的 BLDR）。
GNDV	设备型号版本	标识 DMDL 捆绑包中网格节点设备型号版本的字符串。
GNGP	组	网格节点所属的组（在链路成本和服务查询排名环境中）。
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包中的条目时，都会生成此消息。

GN-R：GNDS 注销

如果某个服务已从 StorageGRID 系统中取消注册有关自身的信息，则 CMN 服务将生成此审核消息。

代码	字段	Description
RSLT	结果	更新请求的结果： <ul style="list-style-type: none"> • SUC：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。

GTed：网格任务已结束

此审核消息表示 CMN 服务已完成指定网格任务的处理，并将此任务移至历史表。如果结果为 SUC，ABRT 或 Rolf，则会显示相应的 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	Description
SID	任务 ID	<p>此字段可唯一标识生成的网格任务，并允许在整个生命周期内对网格任务进行管理。</p> <ul style="list-style-type: none"> • 注意：* 任务 ID 是在生成网格任务时分配的，而不是在提交任务时分配的。给定网格任务可能会提交多次，在这种情况下，"任务 ID" 字段不足以唯一链接已提交，已开始和已结束的审核消息。
RSLT	结果	<p>网格任务的最终状态结果：</p> <ul style="list-style-type: none"> • SUC：已成功完成网格任务。 • ABRT：已中止网格任务，但未出现回滚错误。 • Rolf：网格任务已中止，无法完成回滚过程。 • 取消：用户在启动网格任务之前已取消此任务。 • expr：网格任务在启动之前已过期。 • IVLD：网格任务无效。 • auth：未授权网格任务。 • DUPL：网格任务被拒绝为重复项。

GTST：已启动网格任务

此审核消息指示 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，审核消息会紧跟在网格任务提交消息之后。对于提交到 "Pending" 表中的网格任务，用户启动网格任务时会生成此消息。

代码	字段	Description
SID	任务 ID	此字段可唯一标识生成的网格任务，并允许在任务的整个生命周期内对其进行管理。 <ul style="list-style-type: none"> 注意：* 任务 ID 是在生成网格任务时分配的，而不是在提交任务时分配的。给定网格任务可能会提交多次，在这种情况下，"任务 ID" 字段不足以唯一链接已提交，已开始和已结束的审核消息。
RSLT	结果	结果。此字段只有一个值： <ul style="list-style-type: none"> SUC：已成功启动网格任务。

GTSU：已提交网格任务

此审核消息表示已将网格任务提交到 CMN 服务。

代码	字段	Description
SID	任务 ID	唯一标识生成的网格任务，并允许在整个生命周期内对该任务进行管理。 <ul style="list-style-type: none"> 注意：* 任务 ID 是在生成网格任务时分配的，而不是在提交任务时分配的。给定网格任务可能会提交多次，在这种情况下，"任务 ID" 字段不足以唯一链接已提交，已开始和已结束的审核消息。
TTYP	任务类型	网格任务的类型。
版本	任务版本	指示网格任务版本的数字。
TDSC	任务问题描述	网格任务的用户可读问题描述。
VAT	在时间戳之后有效	网格任务最早有效的时间（从 1970 年 1 月 1 日开始的 UIN64 微秒 - UNIX 时间）。
Vbts	在时间戳之前有效	网格任务有效的最新时间（从 1970 年 1 月 1 日开始的 UIN64 微秒 - UNIX 时间）。

代码	字段	Description
TRC	源	任务源： <ul style="list-style-type: none"> • TXTB：网格任务是以签名文本块的形式通过 StorageGRID 系统提交的。 • 网格：网格任务是通过内部网格任务提交服务提交的。
ACTV	激活类型	激活类型： <ul style="list-style-type: none"> • Auto：已提交网格任务以自动激活。 • PEND：网格任务已提交到待定表中。这是 TXTB 源的唯一可能性。
RSLT	结果	提交结果： <ul style="list-style-type: none"> • SUC：已成功提交网格任务。 • fail：任务已直接移至历史表。

idel：ILM 已启动删除

ILM 开始删除对象时会生成此消息。

在以下任一情况下都会生成 idel 消息：

- * 对于合规 S3 存储分段中的对象 *：当 ILM 开始自动删除对象的过程时，系统会生成此消息，因为该对象的保留期限已过期（假设已启用自动删除设置且已关闭合法保留）。
- * 用于不合规 S3 存储分段或 Swift 容器中的对象 *。ILM 开始删除对象的过程时会生成此消息，因为活动 ILM 策略中的放置说明当前不适用于此对象。

代码	字段	Description
CBID	内容块标识符	对象的 CBID。
CMPA	合规性：自动删除	仅适用于合规 S3 存储分段中的对象。0（false）或 1（true），指示合规对象在保留期限结束时是否应自动删除，除非分段处于合法保留状态。

代码	字段	Description
Cmpl	合规性：法律保留	仅适用于合规 S3 存储分段中的对象。0（false）或 1（true），指示存储分段当前是否处于合法保留状态。
CMPR	合规性：保留期限	仅适用于合规 S3 存储分段中的对象。对象保留期限的长度，以分钟为单位。
CTME	合规性：载入时间	仅适用于合规 S3 存储分段中的对象。对象的载入时间。您可以将保留期限（以分钟为单位）添加到此值，以确定何时可以从存储分段中删除对象。
DMRK	删除标记版本 ID	从版本控制的存储分段中删除对象时创建的删除标记的版本 ID。存储分段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）。
LOC	位置	<p>对象数据在 StorageGRID 系统中的存储位置。如果对象没有位置（例如，已删除），则此对象的值为 ""。</p> <p>CLEC：对于经过纠删编码的对象，应用于对象数据的纠删编码配置文件 ID 和纠删编码组 ID。</p> <p>CLDI：对于复制的对象，LDR 节点 ID 和对象位置的卷 ID。</p> <p>CLNL：归档对象数据时对象位置的弧节点 ID。</p>
路径	S3 存储分段 / 密钥或 Swift 容器 / 对象 ID	S3 存储分段名称和 S3 密钥名称，或 Swift 容器名称和 Swift 对象标识符。
RSLT	结果	<p>ILM 操作的结果。</p> <p>SUC：ILM 操作成功。</p>

代码	字段	Description
规则	规则标签	<ul style="list-style-type: none"> • 如果合规 S3 存储分段中的某个对象因其保留期限已过期而被自动删除，则此字段为空。 • 如果由于当前没有其他应用于对象的放置指令而删除对象，则此字段将显示应用于对象的最后一个 ILM 规则的可读标签。
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。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

LKCU：覆盖对象清理

如果 StorageGRID 删除了先前需要清理以释放存储空间的已覆盖对象，则会生成此消息。当 S3 或 Swift 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进行。

代码	字段	Description
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 存储分段 / 密钥或 Swift 容器 / 对象 ID	S3 存储分段名称和 S3 密钥名称，或 Swift 容器名称和 Swift 对象标识符。
SEGC	容器 UUID	已分段对象的容器的 UUID。只有当对象已分段时，此值才可用。
UUID	通用唯一标识符	仍存在的对象的标识符。只有在尚未删除对象时，此值才可用。

LLST：位置丢失

如果找不到对象副本的位置（复制或擦除编码），则会生成此消息。

代码	字段	Description
CBIL	CBID	受影响的 CBID。
NOID	源节点 ID	丢失位置的节点 ID。
UUID	通用唯一 ID	StorageGRID 系统中受影响对象的标识符。
ECPR	纠删编码配置文件	用于经过擦除编码的对象数据。使用的擦除编码配置文件的 ID。
LTYP	位置类型	CLDI (联机) : 用于复制的对象数据 CLEC (联机) : 用于经过纠删编码的对象数据 CLNL (近线) : 用于归档复制的对象数据
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 (即, 对于复制的对象) 时才返回。 采用的形式 /var/local/rangedb/2/p/13/13/00oJs6X%{h{U}SeUFxE@
RSLT	结果	始终为无。RSLT- 是一个必填消息字段, 但与此消息无关。使用 none 而不是 SUC, 因此不会筛选此消息。
TRC	触发源	User : 用户触发 Syst : 系统已触发

MGAU : 管理审核消息

" 管理 " 类别可将用户请求记录到管理 API。对于 API, 并非 GET 或 HEAD 请求的每个请求都会记录一个响应, 其中包含 API 的用户名, IP 和请求类型。

代码	字段	Description
MDIP	目标 IP 地址	服务器 (目标) IP 地址。

代码	字段	Description
MDNA	域名	主机域名。
MPAT	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	<p>请求正文的内容。虽然默认情况下会记录响应正文，但在某些情况下，如果响应正文为空，则会记录请求正文。由于响应正文中不提供以下信息，因此会从以下 POST 方法的请求正文中获取这些信息：</p> <ul style="list-style-type: none"> • * 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 • 已停用的服务器 ID 位于 * POST /grid/servers/decommission* 中 • 注：* 敏感信息被删除（例如 S3 访问密钥）或用星号屏蔽（例如密码）。
MRmd	请求方法	<p>HTTP 请求方法：</p> <ul style="list-style-type: none"> • 发布 • PUT • 删除 • patch
MRSC	响应代码	响应代码。
MRSP	响应正文	<p>默认情况下，系统会记录响应的内容（响应正文）。</p> <ul style="list-style-type: none"> • 注：* 敏感信息被删除（例如 S3 访问密钥）或用星号屏蔽（例如密码）。

代码	字段	Description
MSIP	源 IP 地址	客户端（源）IP 地址。
MUN	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（SUC）或后端报告的错误。

OLST：系统检测到丢失对象

如果 DDS 服务在 StorageGRID 系统中找不到对象的任何副本，则会生成此消息。

代码	字段	Description
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一个已知直接位置或近线位置。如果卷信息不可用，则只能使用节点 ID 而不使用卷 ID。
路径	S3 存储分段 / 密钥或 Swift 容器 / 对象 ID	如果可用，则为 S3 存储分段名称和 S3 密钥名称，或者 Swift 容器名称和 Swift 对象标识符。
RSLT	结果	此字段的值为 none。RSLT- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC，因此不会筛选此消息。
UUID	通用唯一 ID	StorageGRID 系统中丢失对象的标识符。
卷	卷 ID	如果可用，则为丢失对象的最后一个已知位置的存储节点或归档节点的卷 ID。

ORLM：符合对象规则

如果对象已按照 ILM 规则的指定成功存储和复制，则会生成此消息。



如果策略中的另一条规则使用对象大小高级筛选器，则使用默认的 Make 2 Copies 规则成功存储对象时不会生成 ORLM 消息。

代码	字段	Description
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）。
LOC	位置	<p>对象数据在 StorageGRID 系统中的存储位置。如果对象没有位置（例如，已删除），则此对象的值为 ""。</p> <p>CLEC：对于经过纠删编码的对象，应用于对象数据的纠删编码配置文件 ID 和纠删编码组 ID。</p> <p>CLDI：对于复制的对象，LDR 节点 ID 和对象位置的卷 ID。</p> <p>CLNL：归档对象数据时对象位置的弧节点 ID。</p>
路径	S3 存储分段 / 密钥或 Swift 容器 / 对象 ID	S3 存储分段名称和 S3 密钥名称，或 Swift 容器名称和 Swift 对象标识符。
RSLT	结果	<p>ILM 操作的结果。</p> <p>SUC：ILM 操作成功。</p>
规则	规则标签	为应用于此对象的 ILM 规则提供的可读标签。
SEGC	容器 UUID	已分段对象的容器的 UUID。只有当对象已分段时，此值才可用。
SGCB	容器 CBID	已分段对象的容器的 CBID。只有当对象已分段时，此值才可用。

代码	字段	Description
统计	Status	ILM 操作的状态。 Done：已完成对对象的 ILM 操作。 DDER：对象已标记为待未来 ILM 重新评估。 PRGD：此对象已从 StorageGRID 系统中删除。 NLOC：在 StorageGRID 系统中找不到对象数据。此状态可能表示对象数据的所有副本均缺失或已损坏。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。

可以对单个对象多次发出 ORLM 审核消息。例如，每当发生以下事件之一时都会发出此消息：

- 对象的 ILM 规则将永久满足。
- 此 Epoch 已满足对象的 ILM 规则。
- ILM 规则已删除此对象。
- 后台验证过程检测到复制的对象数据的副本已损坏。StorageGRID 系统会执行 ILM 评估以替换损坏的对象。

相关信息

["对象载入事务"](#)

["对象删除事务"](#)

OVWR：对象覆盖

如果外部（客户端请求的）操作导致一个对象被另一个对象覆盖，则会生成此消息。

代码	字段	Description
CBID	内容块标识符（新增）	新对象的 CBID。
CSIZ	先前对象大小	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。

代码	字段	Description
UUID	通用唯一 ID（新）	StorageGRID 系统中新对象的标识符。
OUID	通用唯一 ID（以前的）	StorageGRID 系统中上一个对象的标识符。
路径	S3 或 Swift 对象路径	用于上一个对象和新对象的 S3 或 Swift 对象路径
RSLT	结果代码	对象覆盖事务的结果。结果始终为： SUC：成功

Sadd：禁用安全审核

此消息指示发起服务（节点 ID）已关闭审核消息日志记录；不再收集或传送审核消息。

代码	字段	Description
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- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC，因此不会筛选此消息。

此消息表示先前已启用日志记录，但现在已禁用。通常，只有在批量载入期间才会使用此功能来提高系统性能。在批量活动之后，将还原审核（SAade），并永久阻止禁用审核的功能。

Sade：启用安全审核

此消息表示发起服务（节点 ID）已还原审核消息日志记录；正在再次收集和传送审核消息。

代码	字段	Description
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	Description
RSLT	结果	此字段的值为 none。RSLT- 是一个必填消息字段，但与此消息无关。使用 none 而不是 SUC，因此不会筛选此消息。

此消息表示先前已禁用日志记录（Sadd），但现在已还原。通常，只有在批量载入期间才会使用此功能来提高系统性能。在批量活动之后，审核将恢复，而禁用审核的功能将被永久阻止。

SCMT：对象存储提交

网格内容在提交之前不可用或无法识别为已存储（这意味着它已持久存储）。持久存储的内容已完全写入磁盘，并已通过相关的完整性检查。将内容块提交到存储时会发出此消息。

代码	字段	Description
CBID	内容块标识符	提交到永久存储的内容块的唯一标识符。
RSLT	结果代码	将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。

SDEL：S3 delete

当 S3 客户端发出删除事务时，系统会请求删除指定的对象或存储分段。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0。存储分段上的操作不包括此字段。
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。
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）。存储分段上的操作不包括此字段。

代码	字段	Description
DMRK	删除标记版本 ID	从版本控制的存储分段中删除对象时创建的删除标记的版本 ID。存储分段上的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 <ul style="list-style-type: none"> 注：* X-Forwarded-For 如果请求中存在此参数、则会自动包含此参数 X-Forwarded-For 值与请求发件人 IP 地址(SAIP审核字段)不同。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，用于指示上次修改对象的时间。
RSLT	结果代码	删除事务的结果。结果始终为： SUC：成功
S3AI	S3 租户帐户 ID（请求发件人）	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（请求发件人）	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 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源（如果适用）。
SACC	S3 租户帐户名称（请求发件人）	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址（请求发件人）	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称（存储分段所有者）	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。

代码	字段	Description
SBAI	S3 租户帐户 ID (存储分段所有者)	目标存储分段所有者的租户帐户 ID。用于标识跨帐户或匿名访问。
SUSR	S3 用户 URN (请求发件人)	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，也可以是 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，以微秒为单位。
TLSIP	可信负载均衡器 IP 地址	如果请求是由受信任的第 7 层负载均衡器路由的，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	已删除对象的特定版本的版本 ID。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

SGET : S3 GET

当 S3 客户端发出 GET 事务时，系统会请求检索对象或列出存储分段中的对象。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0。存储分段上的操作不包括此字段。
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。
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）。存储分段上的操作不包括此字段。

代码	字段	Description
HTRH	HTTP 请求标头	<p>列出配置期间选择的已记录 HTTP 请求标头名称和值。</p> <ul style="list-style-type: none"> 注： * X-Forwarded-For 如果请求中存在此参数、则会自动包含此参数 X-Forwarded-For 值与请求发件人IP地址(SAIP审核字段)不同。
已振铃	范围读取	仅适用于范围读取操作。指示此请求读取的字节数范围。斜杠 (/) 后面的值显示整个对象的大小。
RSLT	结果代码	<p>GET 事务的结果。结果始终为：</p> <p>SUC：成功</p>
S3AI	S3 租户帐户 ID (请求发件人)	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 (请求发件人)	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 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源 (如果适用)。
SACC	S3 租户帐户名称 (请求发件人)	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址 (请求发件人)	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称 (存储分段所有者)	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID (存储分段所有者)	目标存储分段所有者的租户帐户 ID。用于标识跨帐户或匿名访问。

代码	字段	Description
SUSR	S3 用户 URN (请求发件人)	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，也可以是 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，以微秒为单位。
TLSIP	可信负载均衡器 IP 地址	如果请求是由受信任的第 7 层负载均衡器路由的，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	所请求对象的特定版本的版本 ID。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

Shea : S3 机头

当 S3 客户端发出 HEAD 事务时，系统会请求检查是否存在对象或存储分段，并检索有关对象的元数据。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0。存储分段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	检查对象的大小（以字节为单位）。存储分段上的操作不包括此字段。

代码	字段	Description
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注： * X-Forwarded-For 如果请求中存在此参数、则会自动包含此参数 X-Forwarded-For 值与请求发件人IP地址(SAIP审核字段)不同。
RSLT	结果代码	GET 事务的结果。结果始终为： SUC : 成功
S3AI	S3 租户帐户 ID (请求发件人)	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 (请求发件人)	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 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
SACC	S3 租户帐户名称 (请求发件人)	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址 (请求发件人)	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称 (存储分段所有者)	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID (存储分段所有者)	目标存储分段所有者的租户帐户 ID 。用于标识跨帐户或匿名访问。
SUSR	S3 用户 URN (请求发件人)	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，也可以是 LDAP 用户。例如： urn:sgws:identity::03393893651506583485:root 匿名请求为空。

代码	字段	Description
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载均衡器 IP 地址	如果请求是由受信任的第 7 层负载均衡器路由的，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	所请求对象的特定版本的版本 ID。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

SPOS : S3 POST

当S3客户端发出后对象还原请求时、系统会请求将对象从AWS Glacier存储还原到云存储池。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0。
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。
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	列出配置期间选择的已记录 HTTP 请求标头名称和值。 <ul style="list-style-type: none"> 注： * X-Forwarded-For 如果请求中存在此参数、则会自动包含此参数 X-Forwarded-For 值与请求发件人IP地址(SAIP审核字段)不同。
RSLT	结果代码	POST 对象还原请求的结果。结果始终为： SUC : 成功

代码	字段	Description
S3AI	S3 租户帐户 ID (请求发件人)	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 (请求发件人)	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 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源(如果适用)。
SACC	S3 租户帐户名称 (请求发件人)	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址 (请求发件人)	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称 (存储分段所有者)	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID (存储分段所有者)	目标存储分段所有者的租户帐户 ID。用于标识跨帐户或匿名访问。
SRCF	子资源配置	还原信息。
SUSR	S3 用户 URN (请求发件人)	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，也可以是 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，以微秒为单位。
TLSIP	可信负载均衡器 IP 地址	如果请求是由受信任的第 7 层负载均衡器路由的，则为负载均衡器的 IP 地址。

代码	字段	Description
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	所请求对象的特定版本的版本 ID。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

SPUT : S3 PUT

当 S3 客户端发出 PUT 事务时，系统会请求创建新对象或存储分段。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0。存储分段上的操作不包括此字段。
CMPS	合规性设置	创建存储分段时使用的合规性设置（如果 PUT 存储分段请求中存在）（截断为前 1024 个字符）
CNCH	一致性控制标题	如果请求中存在一致性控制 HTTP 请求标头的值。
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）。存储分段上的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 <ul style="list-style-type: none"> 注： * X-Forwarded-For 如果请求中存在此参数、则会自动包含此参数 X-Forwarded-For 值与请求发件人 IP 地址(SAIP 审核字段)不同。
LKEN	对象锁定已启用	请求标头的值 x-amz-bucket-object-lock-enabled(如果 PUT 分段请求中存在)。

代码	字段	Description
LKLH	对象锁定合法保留	请求标头的值 x-amz-object-lock-legal-hold(如果PUT对象请求中存在)。
LKMD	对象锁定保留模式	请求标头的值 x-amz-object-lock-mode(如果PUT对象请求中存在)。
LKRU	对象锁定保留至日期	请求标头的值 x-amz-object-lock-retain-until-date(如果PUT对象请求中存在)。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，用于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： SUC：成功
S3AI	S3 租户帐户 ID (请求发件人)	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 (请求发件人)	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 存储分段	S3 存储分段名称。
S3KY	S3KY	S3 密钥名称，不包括存储分段名称。存储分段上的操作不包括此字段。
S3SR	S3 子资源	要在其上操作的分段或对象子资源(如果适用)。
SACC	S3 租户帐户名称 (请求发件人)	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址 (请求发件人)	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称 (存储分段所有者)	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID (存储分段所有者)	目标存储分段所有者的租户帐户 ID。用于标识跨帐户或匿名访问。

代码	字段	Description
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（请求发件人）	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，也可以是 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，以微秒为单位。
TLSIP	可信负载均衡器 IP 地址	如果请求是由受信任的第 7 层负载均衡器路由的，则为负载均衡器的 IP 地址。
ULID	上传 ID	仅包含在用于完成多部件上传操作的 SPUT 消息中。表示所有部件均已上传和组装。
UUID	通用唯一标识符	StorageGRID 系统中对象的标识符。
VSID	版本 ID	在受版本控制的存储分段中创建的新对象的版本 ID。对未版本控制的分段中的分段和对象执行的操作不包括此字段。
VSST	版本控制状态	存储分段的新版本控制状态。使用两种状态："enabled" 或 "suspended"。对对象执行的操作不包括此字段。

Srem：对象存储删除

从永久性存储中删除内容后会发出此消息，并且无法再通过常规 API 进行访问。

代码	字段	Description
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	Description
RSLT	结果代码	指示内容删除操作的结果。唯一定义的值为： SUC：从永久性存储中删除的内容

此审核消息表示已从节点中删除给定内容块，无法再直接请求。此消息可用于跟踪系统中已删除内容的流。

SUPD：已更新 S3 元数据

当 S3 客户端更新所载入对象的元数据时，S3 API 会生成此消息。如果元数据更新成功，则服务器会发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0。存储分段上的操作不包括此字段。
CNCH	一致性控制标题	更新存储分段的合规性设置时，如果请求中存在一致性控制 HTTP 请求标头的值。
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）。存储分段上的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 • 注：* X-Forwarded-For 如果请求中存在此参数、则会自动包含此参数 X-Forwarded-For 值与请求发件人 IP 地址(SAIP审核字段)不同。
RSLT	结果代码	GET 事务的结果。结果始终为： SUC：成功
S3AI	S3 租户帐户 ID（请求发件人）	发送请求的用户的租户帐户 ID。空值表示匿名访问。

代码	字段	Description
S3AK	S3 访问密钥 ID (请求发件人)	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 存储分段	S3 存储分段名称。
S3KY	S3 密钥	S3 密钥名称, 不包括存储分段名称。存储分段上的操作不包括此字段。
SACC	S3 租户帐户名称 (请求发件人)	发送请求的用户的租户帐户名称。匿名请求为空。
SAIP	IP 地址 (请求发件人)	发出请求的客户端应用程序的 IP 地址。
SBAC	S3 租户帐户名称 (存储分段所有者)	存储分段所有者的租户帐户名称。用于标识跨帐户或匿名访问。
SBAI	S3 租户帐户 ID (存储分段所有者)	目标存储分段所有者的租户帐户 ID。用于标识跨帐户或匿名访问。
SUSR	S3 用户 URN (请求发件人)	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, 也可以是 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, 以微秒为单位。
TLSIP	可信负载均衡器 IP 地址	如果请求是由受信任的第 7 层负载均衡器路由的, 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	已更新其元数据的对象的特定版本的版本 ID。对未版本控制的分段中的分段和对象执行的操作不包括此字段。

SVRF：对象存储验证失败

每当内容块验证过程失败时，都会发出此消息。每次从磁盘读取或写入复制的对象数据时，都会执行多项验证和完整性检查，以确保发送给请求用户的数据与最初载入系统的数据完全相同。如果其中任何一项检查失败，系统会自动隔离损坏的复制对象数据，以防止再次检索该数据。

代码	字段	Description
CBID	内容块标识符	验证失败的内容块的唯一标识符。
RSLT	结果代码	验证失败类型： CRCF：循环冗余检查（CRC）失败。 HMAC：基于哈希的消息身份验证代码（HMAC）检查失败。 EHSB：意外的加密内容哈希。 PHSB：意外的原始内容哈希。 SEQC：磁盘上的数据顺序不正确。 PERR：磁盘文件的结构无效。 DERR：磁盘错误。 fnam：文件名错误。

- 注：* 应密切监控此消息。内容验证失败可能表示尝试篡改内容或即将发生的硬件故障。

要确定哪个操作触发了消息，请参见 amid（模块 ID）字段的值。例如，SV财年 值表示消息是由存储验证程序模块生成的，即后台验证，STor 表示消息是通过内容检索触发的。

SVRU：对象存储验证未知

LDR 服务的存储组件会持续扫描对象存储中复制的对象数据的所有副本。如果在对象存储中检测到复制的对象数据的未知或意外副本并将其移动到隔离目录，则会发出此消息。

代码	字段	Description
FPTH	文件路径	意外对象副本的文件路径。

代码	字段	Description
RSLT	结果	此字段的值为 "无"。RSLT- 是一个必填消息字段，但与此消息无关。使用 "无" 而不是 "CSU"，因此不会筛选此消息。

- 注：* 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意外的对象数据副本。应立即调查这种情况，以确定这些副本是如何创建的，因为这可能表示尝试篡改内容或即将发生硬件故障。

SYSD：节点停止

如果服务正常停止，则会生成此消息以指示已请求关闭。通常，只有在后续重新启动后才会发送此消息，因为在关闭之前未清除审核消息队列。如果服务未重新启动，请查找在关闭序列开始时发送的 SYST 消息。

代码	字段	Description
RSLT	完全关闭	关闭的性质： SUC：系统已完全关闭。

此消息不会指示是否正在停止主机服务器，仅会指示报告服务。SYSD 的 RSLT 不能指示 "异常" 关闭，因为只有 "清理" 关闭才会生成此消息。

Syst：节点正在停止

如果服务正常停止，则会生成此消息，以指示已请求关闭，并且此服务已启动其关闭序列。Syst 可用于确定是否在重新启动服务之前请求关闭（与通常在服务重新启动后发送的 SYSD 不同）。

代码	字段	Description
RSLT	完全关闭	关闭的性质： SUC：系统已完全关闭。

此消息不会指示是否正在停止主机服务器，仅会指示报告服务。SYST 消息的 RSLT 代码不能指示 "异常" 关闭，因为只有 "清理" 关闭才会生成此消息。

SYSU：节点启动

重新启动服务时，系统会生成此消息，以指示上次关闭是正常关闭（已发出命令）还是无序关闭（意外关闭）。

代码	字段	Description
RSLT	完全关闭	关闭的性质： SUC：系统已完全关闭。 DSDN：系统未完全关闭。 VRGN：在安装（或重新安装）服务器后首次启动系统。

此消息不会指示是否已启动主机服务器，仅会指示报告服务。此消息可用于：

- 检测审核跟踪中的不连续性。
- 确定服务在运行期间是否出现故障（因为 StorageGRID 系统的分布式特征可能会掩盖这些故障）。Server Manager 会自动重新启动失败的服务。

VLST：用户启动的卷丢失

每当出现时、都会发出此消息 `/proc/CMSI/Volume_Lost` 命令已运行。

代码	字段	Description
VOLL	卷标识符下限	受影响卷范围的下端或单个卷。
VOLU	卷标识符上限	受影响卷范围的上限。如果只有一个卷，则等于 VOLL。
NOID	源节点 ID	丢失位置的节点 ID。
LTYP	位置类型	"CLDI"（联机）或 "CLNL"（近线）。如果未指定，则默认为 "CLDI"。
RSLT	结果	始终为 "无"。RSLT- 是一个必填消息字段，但与此消息无关。使用 "无" 而不是 "CSU"，因此不会筛选此消息。

WDEL：Swift delete

当 Swift 客户端发出删除事务时，系统会请求删除指定的对象或容器。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0。对容器执行的操作不包括此字段。
CSIZ	内容大小	已删除对象的大小（以字节为单位）。对容器执行的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 <ul style="list-style-type: none"> 注： * X-Forwarded-For 如果请求中存在此参数、则会自动包含此参数 X-Forwarded-For 值与请求发件人 IP 地址(SAIP 审核字段)不同。
MTME	上次修改时间	Unix 时间戳，以微秒为单位，用于指示上次修改对象的时间。
RSLT	结果代码	删除事务的结果。结果始终为： SUC：成功
SAIP	请求客户端的 IP 地址	发出请求的客户端应用程序的 IP 地址。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载均衡器 IP 地址	如果请求是由受信任的第 7 层负载均衡器路由的，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。
WAcc	Swift 帐户 ID	StorageGRID 系统指定的唯一帐户 ID。
WCON	Swift 容器	Swift 容器名称。
WOBJ	Swift 对象	Swift 对象标识符。对容器执行的操作不包括此字段。

代码	字段	Description
WUSR	Swift 帐户用户	用于唯一标识执行事务的客户端的 Swift 帐户用户名。

WGET : Swift GET

当 Swift 客户端发出 GET 事务时，系统会请求检索对象，列出容器中的对象或列出帐户中的容器。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0。对帐户和容器执行的操作不包括此字段。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。对帐户和容器执行的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 <ul style="list-style-type: none"> 注： * X-Forwarded-For 如果请求中存在此参数、则会自动包含此参数 X-Forwarded-For 值与请求发件人 IP 地址(SAIP 审核字段)不同。
RSLT	结果代码	GET 事务的结果。结果始终为 SUC : 成功
SAIP	请求客户端的 IP 地址	发出请求的客户端应用程序的 IP 地址。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载均衡器 IP 地址	如果请求是由受信任的第 7 层负载均衡器路由的，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。

代码	字段	Description
WAcc	Swift 帐户 ID	StorageGRID 系统指定的唯一帐户 ID。
WCON	Swift 容器	Swift 容器名称。对帐户执行的操作不包括此字段。
WOBJ	Swift 对象	Swift 对象标识符。对帐户和容器执行的操作不包括此字段。
WUSR	Swift 帐户用户	用于唯一标识执行事务的客户端的 Swift 帐户用户名。

WHEA : Swift head

当 Swift 客户端发出 HEAD 事务时，系统会请求检查是否存在帐户，容器或对象，并检索任何相关元数据。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0。对帐户和容器执行的操作不包括此字段。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。对帐户和容器执行的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 <ul style="list-style-type: none"> 注：* X-Forwarded-For 如果请求中存在此参数、则会自动包含此参数 X-Forwarded-For 值与请求发件人 IP 地址(SAIP审核字段)不同。
RSLT	结果代码	HEAD 事务的结果。结果始终为： SUC : 成功
SAIP	请求客户端的 IP 地址	发出请求的客户端应用程序的 IP 地址。

代码	字段	Description
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载均衡器 IP 地址	如果请求是由受信任的第 7 层负载均衡器路由的，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。
WAcc	Swift 帐户 ID	StorageGRID 系统指定的唯一帐户 ID。
WCON	Swift 容器	Swift 容器名称。对帐户执行的操作不包括此字段。
WOBJ	Swift 对象	Swift 对象标识符。对帐户和容器执行的操作不包括此字段。
WUSR	Swift 帐户用户	用于唯一标识执行事务的客户端的 Swift 帐户用户名。

WWPUT : Swift PUT

当 Swift 客户端发出 PUT 事务时，系统会请求创建新的对象或容器。如果事务成功，服务器将发出此消息。

代码	字段	Description
CBID	内容块标识符	请求的内容块的唯一标识符。如果 CBID 未知，则此字段将设置为 0。对容器执行的操作不包括此字段。
CSIZ	内容大小	检索到的对象的大小（以字节为单位）。对容器执行的操作不包括此字段。
HTRH	HTTP 请求标头	列出配置期间选择的已记录 HTTP 请求标头名称和值。 <ul style="list-style-type: none"> 注： * X-Forwarded-For 如果请求中存在此参数、则会自动包含此参数 X-Forwarded-For 值与请求发件人 IP 地址(SAIP审核字段)不同。

代码	字段	Description
MTME	上次修改时间	Unix 时间戳，以微秒为单位，用于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： SUC：成功
SAIP	请求客户端的 IP 地址	发出请求的客户端应用程序的 IP 地址。
时间	时间	请求的总处理时间，以微秒为单位。
TLSIP	可信负载均衡器 IP 地址	如果请求是由受信任的第 7 层负载均衡器路由的，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。
WAcc	Swift 帐户 ID	StorageGRID 系统指定的唯一帐户 ID。
WCON	Swift 容器	Swift 容器名称。
WOBJ	Swift 对象	Swift 对象标识符。对容器执行的操作不包括此字段。
WUSR	Swift 帐户用户	用于唯一标识执行事务的客户端的 Swift 帐户用户名。

版权信息

版权所有 © 2024 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。