



## 审核消息格式 StorageGRID software

NetApp  
July 23, 2026

# 目录

- 审核消息格式 ..... 1
  - 了解 StorageGRID 审核消息的结构 ..... 1
  - StorageGRID 审核消息中的数据类型 ..... 1
  - StorageGRID 审核消息中的事件特定数据 ..... 2
  - StorageGRID 审核消息中的常见元素 ..... 3
  - StorageGRID 审核消息格式和示例 ..... 4

# 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(FC32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):9445736326500603516]]
```

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： <ul style="list-style-type: none"> <li>• 反斜杠为 \。</li> <li>• 回车符为 \r。</li> <li>• 双引号为 \"。</li> <li>• 换行符（新行）为 \n。</li> <li>• 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）。</li> </ul> |

## 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。<br><br>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。<br><br>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。                                                                                                                                                                                                                                 |
| 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。<br><br>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):"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):157922414
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):"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，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\): "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):"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):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。

## 版权信息

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

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

## 商标信息

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