审核消息格式

StorageGRID 11.8

NetApp
March 19, 2024

目录

审核消息格式

审核消息格式：概述

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 "审核说明" 和 "审计和" 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。属性元素不会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的值由双引号""括起来。

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；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	长度可变的UTF-8字符数组。可以按照以下约定对字符进行转义： • 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\] \\[时间\(UI64\)
：11454\][SAIP\(iPad\)："10.224.0.100"\][S3AI\(CStr\)："60025621595611246499"\] \[SACC\(CStr\)
："account"\][S3AK\(CStr\)："SGKH4_Nc8SO1H6w3w0nCOFCGk__E6dYzKlumRsKGA="\]
\\[SUSR\(CStr\)："urn：sgws：Identity：：：60025621595611246499：root"\] \\[SBAI\(CStr\)
："60025621595611246499"\\][SBAC\(CStr\)："account"\\][S3BK\(CStr\)："bket"\\] \[S3KY\(CStr\)
："object"\][CBID\(UI64\)：0xCC128B9B9E2283274\] \\[UUUID\(CStr\)："B975D2CE-E4DA-4D14-
8A23-1CB4B83F2CD8"\\[CSEZ\(UI64\)：30720\][aver (UI32)：10] \[ATIM (UI64)
：1543998285921845]\[ATYP\(FC32\)：Shea\][ANID (UI32)：12281045][AMID (FC32)：S3RQ] \[Atid
(UI64)：15552417629170647261]]
```

。 `ATYP` Element (在示例中带下划线)用于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机头请求生成的。

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的四字符标识符。这表示生成审核消息的代码段。
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。显示在中审核消息开头的可供用户读取的时间 `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：要记录的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。

以下是可能显示在中的审核消息示例 `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):"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):"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、该事务会将对象的写入记录到存储分段中。

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\(CSTR\):"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。此值是审核消息本身的ATIM属性的可读版本：

```
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 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。