# Formato da mensagem de auditoria

StorageGRID

NetApp
March 12, 2025

# Índice

# Formato da mensagem de auditoria

As mensagens de auditoria trocadas no sistema StorageGRID incluem informações padrão comuns a todas as mensagens e conteúdo específico que descreve o evento ou a atividade que está sendo relatada.

Se as informações resumidas fornecidas pelas `audit-explain` ferramentas e `audit-sum` forem insuficientes, consulte esta secção para compreender o formato geral de todas as mensagens de auditoria.

A seguir está um exemplo de mensagem de auditoria como ela pode aparecer no arquivo de log de auditoria:

```
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]]
```

Cada mensagem de auditoria contém uma cadeia de elementos de atributo. Toda a cadeia de carateres está entre colchetes (`[ ]`), e cada elemento de atributo na cadeia de carateres tem as seguintes caraterísticas:

- Entre os suportes `[ ]`
- Introduzido pela cadeia de carateres `AUDT`, que indica uma mensagem de auditoria
- Sem delimitadores (sem vírgulas ou espaços) antes ou depois
- Terminado por um caractere de alimentação de linha `\n`

Cada elemento inclui um código de atributo, um tipo de dados e um valor que são relatados neste formato:

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

O número de elementos de atributo na mensagem depende do tipo de evento da mensagem. Os elementos de atributo não são listados em nenhuma ordem específica.

A lista a seguir descreve os elementos do atributo:

- `ATTR` é um código de quatro carateres para o atributo que está sendo relatado. Existem alguns atributos que são comuns a todas as mensagens de auditoria e outros que são específicos para eventos.
- `type` É um identificador de quatro carateres do tipo de dados de programação do valor, como UI64, FC32 e assim por diante. O tipo está entre parênteses `( )`.
- `value` é o conteúdo do atributo, normalmente um valor numérico ou de texto. Os valores seguem sempre dois pontos (`:`). Os valores do tipo de dados CSTR são cercados por aspas `'" "`duplas .

**Informações relacionadas**

Utilize a ferramenta de auditoria-explicação

Use a ferramenta audit-sum

# Tipos de dados

Diferentes tipos de dados são usados para armazenar informações em mensagens de auditoria.

| Tipo | Descrição |
|---|---|
| UI32 | Inteiro longo não assinado (32 bits); ele pode armazenar os números de 0 a 4.294.967.295. |
| UI64 | Número inteiro duplo longo não assinado (64 bits); pode armazenar os números de 0 a 18.446.744.073.709.551.615. |
| FC32 | Constante de quatro carateres; um valor inteiro não assinado de 32 bits representado como quatro carateres ASCII, como "ABCD". |
| IPAD | Usado para endereços IP. |
| CSTR | Um array de comprimento variável de carateres UTF -8. Os carateres podem ser escapados com as seguintes convenções:<br>• Barra invertida é.<br>• O retorno do carro é r.<br>• Aspas duplas.<br>• A alimentação de linha (nova linha) é n.<br>• Os carateres podem ser substituídos por seus equivalentes hexadecimais (no formato HH, onde HH é o valor hexadecimal que representa o caractere). |

# Dados específicos do evento

Cada mensagem de auditoria no log de auditoria Registra dados específicos para um evento do sistema.

Após o contentor de abertura `[AUDT:` que identifica a própria mensagem, o próximo conjunto de atributos fornece informações sobre o evento ou ação descrito pela mensagem de auditoria. Esses atributos são

destacados no exemplo a seguir:

```
2018 11454 S3AI SGKH4 6002562159561124649 9 UI64-12 10.224.0 6002562159561124649
E6DYZKLUMRSKJA S3BK-05T08:24 100 S3AK 6002562159561124649 S3KY
[AUDT:*[RSLT(FC32):SUCS]* *[TIME STR(UI64):45,921845 E4DA UI64 30720 UI32 10 UI64
1543998285921845 FC32 UI32 12281045 FC32 S3RQ UI64 15552417629170647261
```

O `ATYP` elemento (sublinhado no exemplo) identifica qual evento gerou a mensagem. Esta mensagem de exemplo inclui o código de mensagem SHEA ([ATYP(FC32):SHEA]), indicando que foi gerado por uma solicitação DE CABEÇALHO S3 bem-sucedida.

**Informações relacionadas**

Elementos comuns em mensagens de auditoria

Auditar mensagens

# Elementos comuns em mensagens de auditoria

Todas as mensagens de auditoria contêm os elementos comuns.

| Código | Tipo | Descrição |
|---|---|---|
| NO MEIO | FC32 | ID do módulo: Um identificador de quatro carateres do ID do módulo que gerou a mensagem. Isso indica o segmento de código no qual a mensagem de auditoria foi gerada. |
| ANID | UI32 | ID do nó: O ID do nó da grade atribuído ao serviço que gerou a mensagem. Cada serviço recebe um identificador exclusivo no momento em que o sistema StorageGRID é configurado e instalado. Este ID não pode ser alterado. |
| ASES | UI64 | Identificador de sessão de auditoria: Em versões anteriores, este elemento indicou o momento em que o sistema de auditoria foi inicializado após o início do serviço. Este valor de tempo foi medido em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1 de janeiro de 1970).<br><br>**Nota:** este elemento está obsoleto e não aparece mais nas mensagens de auditoria. |
| ASQN | UI64 | Contagem de sequência: Em versões anteriores, esse contador foi incrementado para cada mensagem de auditoria gerada no nó de grade (ANID) e redefinido para zero na reinicialização do serviço.<br><br>**Nota:** este elemento está obsoleto e não aparece mais nas mensagens de auditoria. |
| ATID | UI64 | ID de rastreamento: Um identificador que é compartilhado pelo conjunto de mensagens que foram acionadas por um único evento. |

| Código | Tipo | Descrição |
|---|---|---|
| ATIM | UI64 | Timestamp: A hora em que o evento foi gerado, que acionou a mensagem de auditoria, medida em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1 de janeiro de 1970). Observe que a maioria das ferramentas disponíveis para converter o carimbo de data/hora para data e hora locais são baseadas em milissegundos.<br><br>Pode ser necessário arredondar ou truncar o carimbo de data/hora registado. O tempo legível por humanos que aparece no início da mensagem de auditoria no `audit.log` arquivo é o atributo ATIM no formato ISO 8601. A data e a hora são representadas como *`YYYY-MMDDTHH:MM:SS.UUUUUU`*, onde o `T` é um caractere de cadeia de carateres literal indicando o início do segmento de tempo da data. *`UUUUUU`* são microssegundos. |
| ATYP | FC32 | Tipo de evento: Um identificador de quatro carateres do evento que está sendo registrado. Isso rege o conteúdo "payload" da mensagem: Os atributos que estão incluídos. |
| AVER | UI32 | Versão: A versão da mensagem de auditoria. À medida que o software StorageGRID evolui, novas versões de serviços podem incorporar novos recursos em relatórios de auditoria. Este campo permite a compatibilidade retroativa no serviço AMS para processar mensagens de versões mais antigas de serviços. |
| RSLT | FC32 | Resultado: O resultado de evento, processo ou transação. Se não for relevante para uma mensagem, NENHUM será usado em vez DE SUCS para que a mensagem não seja filtrada acidentalmente. |

# Exemplos de mensagens de auditoria

Você pode encontrar informações detalhadas em cada mensagem de auditoria. Todas as mensagens de auditoria usam o mesmo formato.

A seguir está uma mensagem de auditoria de exemplo, como ela pode aparecer no `audit.log` arquivo:

```
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]]
```

A mensagem de auditoria contém informações sobre o evento que está sendo gravado, bem como informações sobre a própria mensagem de auditoria.

Para identificar qual evento é gravado pela mensagem de auditoria, procure o atributo ATYP (destacado abaixo):

```
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]]
```

O valor do atributo ATYP é SPUT. O SPUT representa uma transação S3 PUT, que Registra a ingestão de um objeto em um bucket.

A seguinte mensagem de auditoria também mostra o intervalo ao qual o objeto está associado:

```
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]]
```

Para descobrir quando o evento PUT ocorreu, observe o carimbo de data/hora Universal coordenada (UTC) no início da mensagem de auditoria. Este valor é uma versão legível por humanos do atributo ATIM da própria mensagem de auditoria:

```
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 Registra o tempo, em microssegundos, desde o início da época UNIX. No exemplo, o valor `1405631878959669` é traduzido para Quinta-feira, 17-Jul-2014 21:17:59 UTC.

**Informações relacionadas**

SPUT: S3 PUT

## Elementos comuns em mensagens de auditoria

## Informações sobre direitos autorais



## Informações sobre marcas comerciais