



Formato da mensagem de auditoria

StorageGRID

NetApp
March 12, 2025

Índice

- Formato da mensagem de auditoria 1
 - Formato da mensagem de auditoria: Visão geral 1
 - Tipos de dados 2
 - Dados específicos do evento 2
 - Elementos comuns em mensagens de auditoria 3
 - Exemplos de mensagens de auditoria 4

Formato da mensagem de auditoria

Formato da mensagem de auditoria: Visão geral

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 "auditoria-explicar" ferramentas e "soma de auditoria" 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(FC32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):9445736326500603516]]
```

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

- Entre os suportes []
- Introduzido pela cadeia de caracteres 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 caracteres 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 caracteres 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 .

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 caracteres; um valor inteiro não assinado de 32 bits representado como quatro caracteres ASCII, como "ABCD".
IPAD	Usado para endereços IP.
CSTR	Um array de comprimento variável de caracteres UTF-8. Os caracteres podem ser escapados com as seguintes convenções: <ul style="list-style-type: none">• Barra invertida é.• O retorno do carro é r.• Aspas duplas.• A alimentação de linha (nova linha) é n.• Os caracteres 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 conteúdo 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 60025621595611246499 UI64-12 10.224.0 60025621595611246499
E6DYZKLUMRSKJA S3BK-05T08:24 100 S3AK 60025621595611246499 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 "SHEA" código de mensagem ([ATYP(FC32):SHEA]), indicando que foi gerado por uma solicitação DE CABEÇALHO S3 bem-sucedida.

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 caracteres 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. Esta ID não pode ser alterada.
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). 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. 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.
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. 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 <code>audit.log</code> arquivo é o atributo ATIM no formato ISO 8601. A data e a hora são representadas como <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code> , onde o <code>T</code> é um caractere de cadeia de caracteres literal indicando o início do segmento de tempo da data. <code>UUUUUU</code> são microssegundos.

Código	Tipo	Descrição
ATYP	FC32	Tipo de evento: Um identificador de quatro caracteres 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):"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]]
```

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):"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]]
```

O valor do atributo ATYP é SPUT. "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\):"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]]
```

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):"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 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 sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.