Revisar logs de auditoria

StorageGRID software

NetApp
December 03, 2025

Índice

Revisar logs de auditoria

Mensagens e logs de auditoria

Estas instruções contêm informações sobre a estrutura e o conteúdo das mensagens de auditoria e dos logs de auditoria do StorageGRID . Você pode usar essas informações para ler e analisar a trilha de auditoria da atividade do sistema.

Estas instruções são para administradores responsáveis por produzir relatórios de atividade e uso do sistema que exigem análise das mensagens de auditoria do sistema StorageGRID .

Para usar o arquivo de log de texto, você deve ter acesso ao compartilhamento de auditoria configurado no nó de administração.

Para obter informações sobre como configurar níveis de mensagens de auditoria e usar um servidor syslog externo, consulte"Configurar mensagens de auditoria e destinos de log" .

Fluxo e retenção de mensagens de auditoria

Todos os serviços do StorageGRID geram mensagens de auditoria durante a operação normal do sistema. Você deve entender como essas mensagens de auditoria se movem pelo sistema StorageGRID para o `audit.log` arquivo.

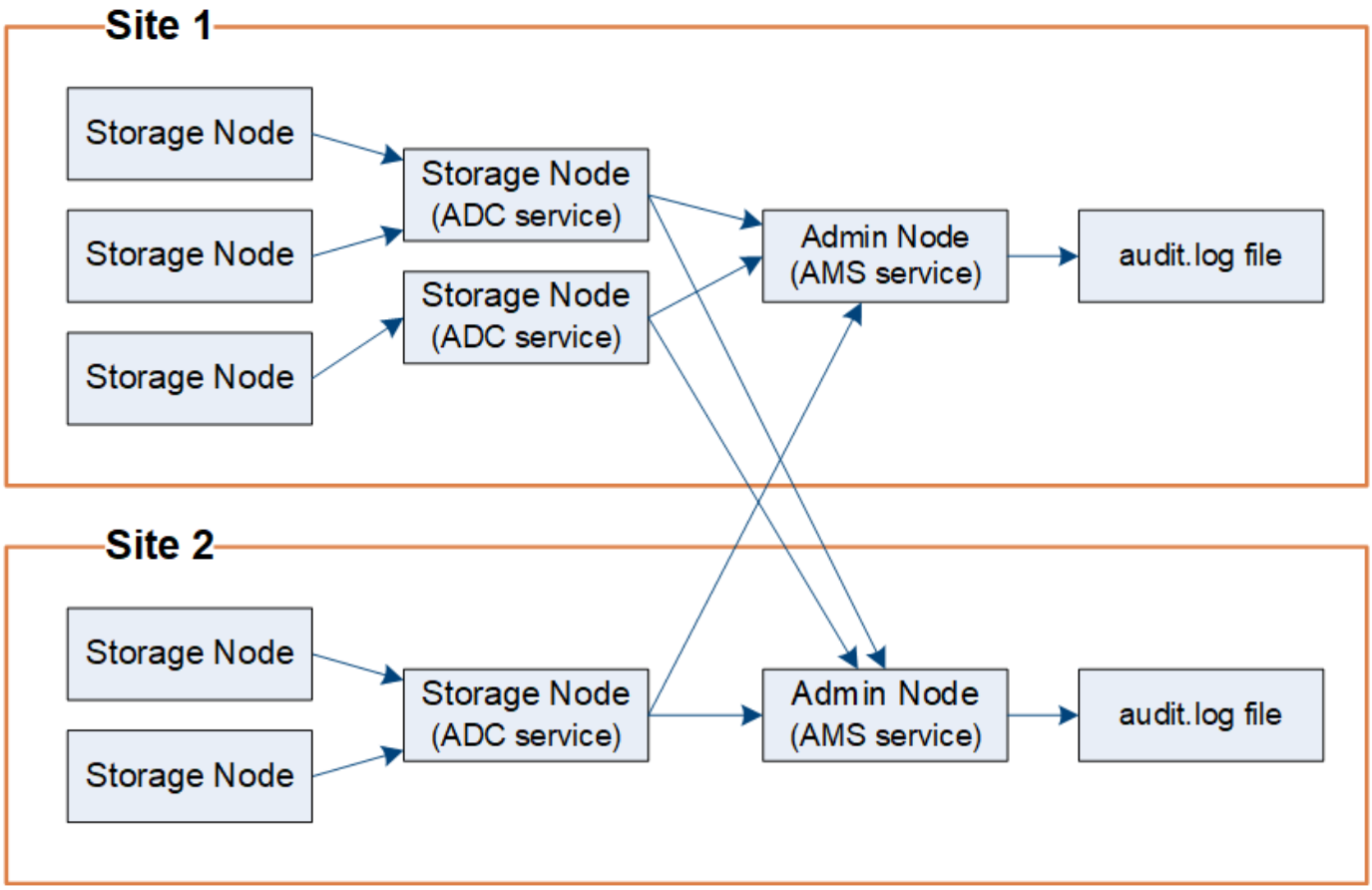
Fluxo de mensagens de auditoria

As mensagens de auditoria são processadas pelos nós de administração e pelos nós de armazenamento que têm um serviço de controlador de domínio administrativo (ADC).

Conforme mostrado no diagrama de fluxo de mensagens de auditoria, cada nó StorageGRID envia suas mensagens de auditoria para um dos serviços do ADC no site do data center. O serviço ADC é habilitado automaticamente para os três primeiros nós de armazenamento instalados em cada site.

Por sua vez, cada serviço ADC atua como um retransmissor e envia sua coleção de mensagens de auditoria para cada nó administrativo no sistema StorageGRID , o que fornece a cada nó administrativo um registro completo da atividade do sistema.

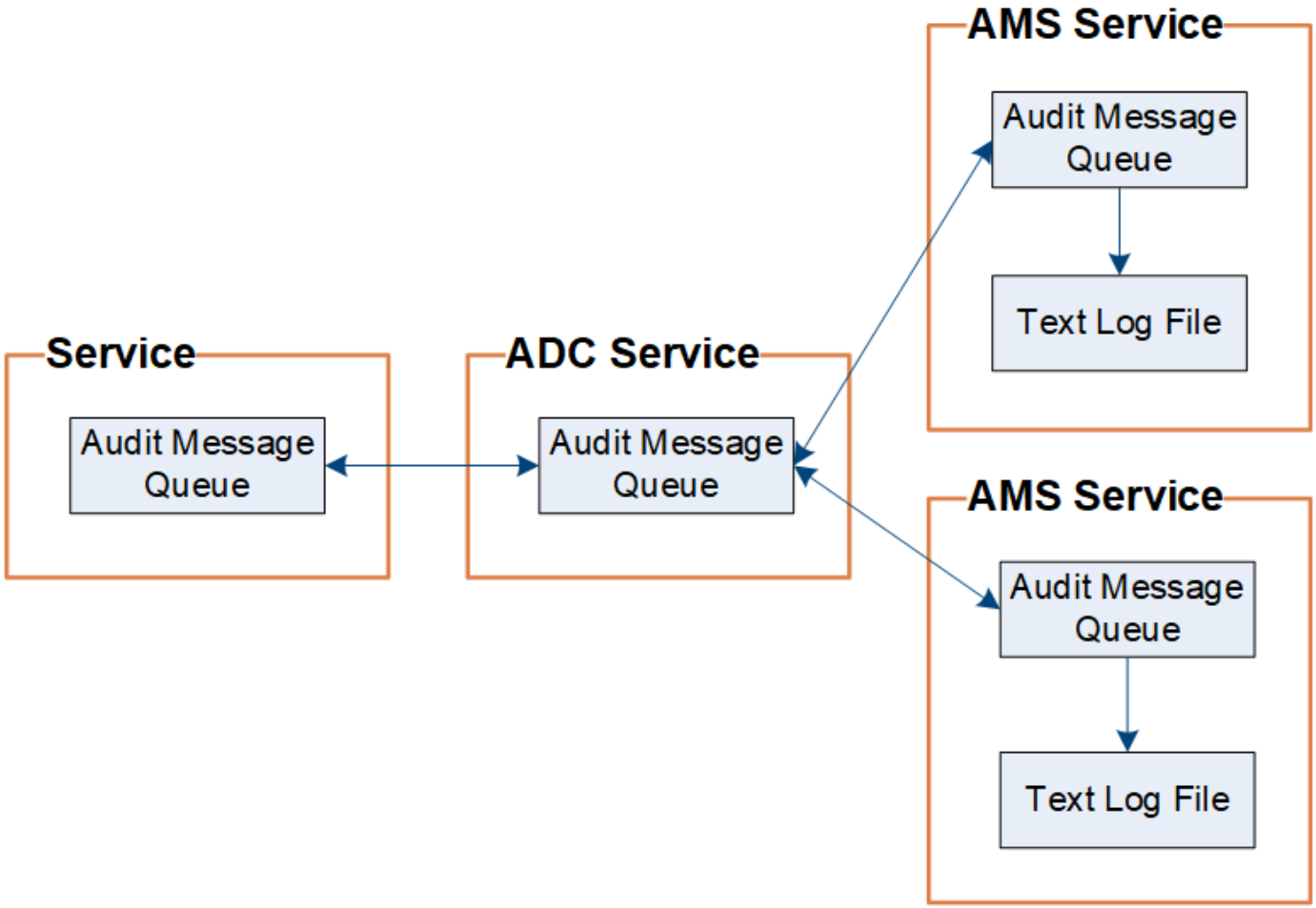
Cada nó de administração armazena mensagens de auditoria em arquivos de log de texto; o arquivo de log ativo é denominado `audit.log` .



Retenção de mensagens de auditoria

O StorageGRID usa um processo de copiar e excluir para garantir que nenhuma mensagem de auditoria seja perdida antes de ser gravada no log de auditoria.

Quando um nó gera ou retransmite uma mensagem de auditoria, a mensagem é armazenada em uma fila de mensagens de auditoria no disco do sistema do nó da grade. Uma cópia da mensagem é sempre mantida em uma fila de mensagens de auditoria até que a mensagem seja gravada no arquivo de log de auditoria no nó de administração. `/var/local/log` diretório. Isso ajuda a evitar a perda de uma mensagem de auditoria durante o transporte.



A fila de mensagens de auditoria pode aumentar temporariamente devido a problemas de conectividade de rede ou capacidade de auditoria insuficiente. À medida que as filas aumentam, elas consomem mais espaço disponível em cada nó `/var/local/` diretório. Se o problema persistir e o diretório de mensagens de auditoria de um nó ficar muito cheio, os nós individuais priorizarão o processamento de seu backlog e ficarão temporariamente indisponíveis para novas mensagens.

Especificamente, você pode ver os seguintes comportamentos:

- Se o `/var/local/log` o diretório usado por um nó de administração ficar cheio, o nó de administração será sinalizado como indisponível para novas mensagens de auditoria até que o diretório não esteja mais cheio. As solicitações do cliente S3 não são afetadas. O alarme XAMS (Repositórios de auditoria inacessíveis) é acionado quando um repositório de auditoria fica inacessível.
- Se o `/var/local/` o diretório usado por um nó de armazenamento com o serviço ADC ficar 92% cheio, o nó será sinalizado como indisponível para mensagens de auditoria até que o diretório esteja apenas 87% cheio. As solicitações do cliente S3 para outros nós não são afetadas. O alarme NRLY (Relés de auditoria disponíveis) é acionado quando os relés de auditoria estão inacessíveis.

> Se não houver nós de armazenamento disponíveis com o serviço ADC, os nós de armazenamento armazenam as mensagens de auditoria localmente no `/var/local/log/localaudit.log` arquivo.

- Se o `/var/local/` diretório usado por um nó de armazenamento ficar 85% cheio, o nó começará a recusar solicitações de cliente S3 com `503 Service Unavailable`.

Os seguintes tipos de problemas podem fazer com que as filas de mensagens de auditoria fiquem muito grandes:

- A interrupção de um nó de administração ou de um nó de armazenamento com o serviço ADC. Se um dos nós do sistema estiver inativo, os nós restantes poderão ficar acumulados.
- Uma taxa de atividade sustentada que excede a capacidade de auditoria do sistema.
- O `/var/local/` espaço em um nó de armazenamento ADC ficando cheio por motivos não relacionados a mensagens de auditoria. Quando isso acontece, o nó para de aceitar novas mensagens de auditoria e prioriza seu backlog atual, o que pode causar backlogs em outros nós.

Alerta de fila de auditoria grande e alarme de mensagens de auditoria na fila (AMQS)

Para ajudar você a monitorar o tamanho das filas de mensagens de auditoria ao longo do tempo, o alerta **Fila de auditoria grande** e o alarme AMQS legado são acionados quando o número de mensagens em uma fila de nó de armazenamento ou fila de nó de administração atinge determinados limites.

Se o alerta **Grande fila de auditoria** ou o alarme AMQS legado for acionado, comece verificando a carga no sistema. Se houver um número significativo de transações recentes, o alerta e o alarme deverão ser resolvidos com o tempo e poderão ser ignorados.

Se o alerta ou alarme persistir e aumentar em gravidade, visualize um gráfico do tamanho da fila. Se o número estiver aumentando constantemente ao longo de horas ou dias, a carga de auditoria provavelmente excedeu a capacidade de auditoria do sistema. Reduza a taxa de operação do cliente ou diminua o número de mensagens de auditoria registradas alterando o nível de auditoria para Gravações do Cliente e Leituras do Cliente para Erro ou Desligado. Ver "Configurar mensagens de auditoria e destinos de log" .

Mensagens duplicadas

O sistema StorageGRID adota uma abordagem conservadora caso ocorra uma falha de rede ou nó. Por esse motivo, podem existir mensagens duplicadas no log de auditoria.

Arquivo de log de auditoria de acesso

O compartilhamento de auditoria contém o ativo `audit.log` arquivo e quaisquer arquivos de log de auditoria compactados. Você pode acessar arquivos de log de auditoria diretamente da linha de comando do nó de administração.

Antes de começar

- Você tem"permissões de acesso específicas" .
- Você deve ter o `Passwords.txt` arquivo.
- Você deve saber o endereço IP de um nó de administração.

Passos

1. Efetue login em um nó de administração:
   a. Digite o seguinte comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Digite a senha listada no `Passwords.txt` arquivo.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no `Passwords.txt` arquivo.

Quando você está logado como root, o prompt muda de `$` para `#` .

2. Vá para o diretório que contém os arquivos de log de auditoria:

```
cd /var/local/log
```

3. Visualize o arquivo de log de auditoria atual ou salvo, conforme necessário.

Rotação do arquivo de log de auditoria

Os arquivos de logs de auditoria são salvos em um nó de administração `/var/local/log` diretório. Os arquivos de log de auditoria ativos são nomeados `audit.log` .

> Opcionalmente, você pode alterar o destino dos logs de auditoria e enviar informações de auditoria para um servidor syslog externo. Os logs locais dos registros de auditoria continuam sendo gerados e armazenados quando um servidor syslog externo é configurado. Ver "Configurar mensagens de auditoria e destinos de log" .

Uma vez por dia, o ativo `audit.log` o arquivo é salvo e um novo `audit.log` o arquivo é iniciado. O nome do arquivo salvo indica quando ele foi salvo, no formato *`yyyy-mm-dd.txt`* . Se mais de um log de auditoria for criado em um único dia, os nomes dos arquivos usarão a data em que o arquivo foi salvo, anexada por um número, no formato *`yyyy-mm-dd.txt.n`* . Por exemplo, `2018-04-15.txt` e `2018-04-15.txt.1` são o primeiro e o segundo arquivos de log criados e salvos em 15 de abril de 2018.

Após um dia, o arquivo salvo é compactado e renomeado, no formato *`yyyy-mm-dd.txt.gz`* , que preserva a data original. Com o tempo, isso resulta no consumo de armazenamento alocado para logs de auditoria no nó de administração. Um script monitora o consumo de espaço do log de auditoria e exclui os arquivos de log conforme necessário para liberar espaço no `/var/local/log` diretório. Os logs de auditoria são excluídos com base na data em que foram criados, sendo os mais antigos excluídos primeiro. Você pode monitorar as ações do script no seguinte arquivo: `/var/local/log/manage-audit.log` .

Este exemplo mostra o ativo `audit.log` arquivo, arquivo do dia anterior(`2018-04-15.txt`), e o arquivo compactado do dia anterior(`2018-04-14.txt.gz`).

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

Formato de arquivo de log de auditoria

Formato de arquivo de log de auditoria

Os arquivos de log de auditoria são encontrados em cada nó administrativo e contêm uma coleção de mensagens de auditoria individuais.

Cada mensagem de auditoria contém o seguinte:

- O Tempo Universal Coordenado (UTC) do evento que disparou a mensagem de auditoria (ATIM) no formato ISO 8601, seguido por um espaço:

  YYYY-MM-DDTHH:MM:SS.UUUUUU, onde *UUUUUU* são microssegundos.

- A própria mensagem de auditoria, entre colchetes e começando com `AUDT` .

O exemplo a seguir mostra três mensagens de auditoria em um arquivo de log de auditoria (quebras de linha adicionadas para facilitar a leitura). Essas mensagens foram geradas quando um locatário criou um bucket S3 e adicionou dois objetos a esse bucket.

```
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::17530064241597054
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::17530064241597054
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::17530064241597054
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]]
```

No formato padrão, as mensagens de auditoria nos arquivos de log de auditoria não são fáceis de ler ou interpretar. Você pode usar o"ferramenta audit-explain" para obter resumos simplificados das mensagens de auditoria no log de auditoria. Você pode usar o"ferramenta de soma de auditoria" para resumir quantas operações de gravação, leitura e exclusão foram registradas e quanto tempo essas operações levaram.

Use a ferramenta audit-explain

Você pode usar o `audit-explain` ferramenta para traduzir as mensagens de auditoria no log de auditoria para um formato fácil de ler.

Antes de começar

- Você tem"permissões de acesso específicas" .
- Você deve ter o `Passwords.txt` arquivo.
- Você deve saber o endereço IP do nó de administração primário.

Sobre esta tarefa

O `audit-explain` A ferramenta, disponível no nó de administração principal, fornece resumos simplificados das mensagens de auditoria em um log de auditoria.

> O `audit-explain` A ferramenta destina-se principalmente ao uso pelo suporte técnico durante operações de solução de problemas. Processamento `audit-explain` consultas podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID .

Este exemplo mostra a saída típica do `audit-explain` ferramenta. Esses quatro"CUSPIR" mensagens de auditoria foram geradas quando o locatário do S3 com ID de conta 92484777680322627870 usou solicitações S3 PUT para criar um bucket chamado "bucket1" e adicionar três objetos a esse bucket.

```
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
```

O `audit-explain` ferramenta pode fazer o seguinte:

- Processe logs de auditoria simples ou compactados. Por exemplo:

  ```
  audit-explain audit.log

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

- Processe vários arquivos simultaneamente. Por exemplo:

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/log/*
  ```

- Aceitar entrada de um pipe, o que permite filtrar e pré-processar a entrada usando o `grep` comando ou outros meios. Por exemplo:

  ```
  grep SPUT audit.log | audit-explain

  grep bucket-name audit.log | audit-explain
  ```

Como os logs de auditoria podem ser muito grandes e lentos para analisar, você pode economizar tempo

filtrando as partes que deseja examinar e executando `audit-explain` nas partes, em vez do arquivo inteiro.

> O `audit-explain` a ferramenta não aceita arquivos compactados como entrada canalizada. Para processar arquivos compactados, forneça seus nomes de arquivo como argumentos de linha de comando ou use o `zcat` ferramenta para descompactar os arquivos primeiro. Por exemplo:
>
> ```
> zcat audit.log.gz | audit-explain
> ```

Use o `help (-h)` opção para ver as opções disponíveis. Por exemplo:

```
$ audit-explain -h
```

Passos

1. Efetue login no nó de administração principal:
   a. Digite o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Digite a senha listada no `Passwords.txt` arquivo.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no `Passwords.txt` arquivo.

   Quando você está logado como root, o prompt muda de `$` para `#` .
2. Digite o seguinte comando, onde `/var/local/log/audit.log` representa o nome e o local do arquivo ou arquivos que você deseja analisar:

   ```
   $ audit-explain /var/local/log/audit.log
   ```

   O `audit-explain` A ferramenta imprime interpretações legíveis por humanos de todas as mensagens no arquivo ou arquivos especificados.

   > Para reduzir o comprimento das linhas e facilitar a leitura, os registros de data e hora não são exibidos por padrão. Se você quiser ver os carimbos de data/hora, use o carimbo de data/hora(`-t`) opção.

Use a ferramenta audit-sum

Você pode usar o `audit-sum` ferramenta para contar as mensagens de auditoria de gravação, leitura, cabeçalho e exclusão e para ver o tempo mínimo, máximo e médio (ou tamanho) para cada tipo de operação.

Antes de começar

- Você tem"permissões de acesso específicas" .
- Você deve ter o `Passwords.txt` arquivo.
- Você deve saber o endereço IP do nó de administração primário.

Sobre esta tarefa

O `audit-sum` A ferramenta, disponível no nó de administração principal, resume quantas operações de

gravação, leitura e exclusão foram registradas e quanto tempo essas operações levaram.

> O `audit-sum` A ferramenta destina-se principalmente ao uso pelo suporte técnico durante operações de solução de problemas. Processamento `audit-sum` consultas podem consumir uma grande quantidade de energia da CPU, o que pode afetar as operações do StorageGRID .

Este exemplo mostra a saída típica do `audit-sum` ferramenta. Este exemplo mostra quanto tempo demoraram as operações do protocolo.

```
  message group           count     min(sec)        max(sec)
average(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
```

O `audit-sum` A ferramenta fornece contagens e tempos para as seguintes mensagens de auditoria do S3, Swift e ILM em um log de auditoria.

> Os códigos de auditoria são removidos do produto e da documentação, pois os recursos são descontinuados. Se você encontrar um código de auditoria que não esteja listado aqui, verifique as versões anteriores deste tópico para versões mais antigas do SG. Por exemplo, "Documentação da ferramenta de soma de auditoria do StorageGRID 11.8" .

Código	Descrição	Consulte
IDEL	Exclusão iniciada pelo ILM: registra quando o ILM inicia o processo de exclusão de um objeto.	"IDEL: Exclusão iniciada pelo ILM"
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou bucket.	"SDEL: S3 EXCLUIR"
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket.	"SGET: S3 OBTER"
KARITÉ	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	"SHEA: CABEÇA S3"
CUSPIR	S3 PUT: Registra uma transação bem-sucedida para criar um novo objeto ou bucket.	"SPUT: S3 PUT"

Código	Descrição	Consulte
WDEL	Swift DELETE: Registra uma transação bem-sucedida para excluir um objeto ou contêiner.	"WDEL: Swift EXCLUIR"
WGET	Swift GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um contêiner.	"WGET: GET rápido"
WHEA	Swift HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou contêiner.	"WHEA: CABEÇA Rápida"
WPUT	Swift PUT: Registra uma transação bem-sucedida para criar um novo objeto ou contêiner.	"WPUT: PUT rápido"

O `audit-sum` ferramenta pode fazer o seguinte:

- Processe logs de auditoria simples ou compactados. Por exemplo:

```
audit-sum audit.log

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

- Processe vários arquivos simultaneamente. Por exemplo:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/log/*
```

- Aceitar entrada de um pipe, o que permite filtrar e pré-processar a entrada usando o `grep` comando ou outros meios. Por exemplo:

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

> Esta ferramenta não aceita arquivos compactados como entrada canalizada. Para processar arquivos compactados, forneça seus nomes de arquivo como argumentos de linha de comando ou use o `zcat` ferramenta para descompactar os arquivos primeiro. Por exemplo:
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

Você pode usar opções de linha de comando para resumir operações em buckets separadamente de operações em objetos ou para agrupar resumos de mensagens por nome de bucket, por período de tempo ou por tipo de destino. Por padrão, os resumos mostram o tempo mínimo, máximo e médio de operação, mas você pode usar o `size (-s)` opção para olhar o tamanho do objeto.

Use o `help (-h)` opção para ver as opções disponíveis. Por exemplo:

```
$ audit-sum -h
```

Passos

1. Efetue login no nó de administração principal:
   a. Digite o seguinte comando: `ssh admin@primary_Admin_Node_IP`
   b. Digite a senha listada no `Passwords.txt` arquivo.
   c. Digite o seguinte comando para alternar para root: `su -`
   d. Digite a senha listada no `Passwords.txt` arquivo.

   Quando você está logado como root, o prompt muda de `$` para `#` .

2. Se você quiser analisar todas as mensagens relacionadas às operações de gravação, leitura, cabeçalho e exclusão, siga estas etapas:
   a. Digite o seguinte comando, onde `/var/local/log/audit.log` representa o nome e o local do arquivo ou arquivos que você deseja analisar:

   ```
   $ audit-sum /var/local/log/audit.log
   ```

   Este exemplo mostra a saída típica do `audit-sum` ferramenta. Este exemplo mostra quanto tempo demoraram as operações do protocolo.

   ```
     message group           count     min(sec)        max(sec)
   average(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
   ```

   Neste exemplo, as operações SGET (S3 GET) são as mais lentas, em média, com 1,13 segundos, mas as operações SGET e SPUT (S3 PUT) mostram tempos longos de pior caso, de cerca de 1.770 segundos.

   b. Para mostrar as 10 operações de recuperação mais lentas, use o comando grep para selecionar apenas mensagens SGET e adicione a opção de saída longa(`-l`) para incluir caminhos de objetos:

   ```
   grep SGET audit.log | audit-sum -l
   ```

   Os resultados incluem o tipo (objeto ou bucket) e o caminho, o que permite que você pesquise no log

de auditoria outras mensagens relacionadas a esses objetos específicos.

```
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/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-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
```

+ A partir deste exemplo de saída, você pode ver que as três solicitações GET do S3 mais lentas foram para objetos com cerca de 5 GB de tamanho, o que é muito maior do que os outros objetos. O tamanho grande é responsável pelos tempos de recuperação lentos no pior caso.

3. Se você quiser determinar quais tamanhos de objetos estão sendo ingeridos e recuperados de sua grade, use a opção de tamanho(`-s`):

   ```
   audit-sum -s audit.log
   ```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                   213371        0.000          10.504
1.695
  SGET                   201906        0.000        5000.000
14.920
  SHEA                    22716        0.001          10.504
2.967
  SPUT                 1771398        0.000        5000.000
2.495
```

Neste exemplo, o tamanho médio do objeto para SPUT é inferior a 2,5 MB, mas o tamanho médio para SGET é muito maior. O número de mensagens SPUT é muito maior que o número de mensagens SGET, indicando que a maioria dos objetos nunca é recuperada.

4. Se você quiser determinar se as recuperações foram lentas ontem:

   a. Emita o comando no log de auditoria apropriado e use a opção group-by-time(`-gt`), seguido pelo período de tempo (por exemplo, 15M, 1H, 10S):

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

Esses resultados mostram que o tráfego S3 GET atingiu o pico entre 06:00 e 07:00. Os tempos máximo e médio também são consideravelmente maiores nesses momentos e não aumentam gradualmente conforme a contagem aumenta. Isso sugere que a capacidade foi excedida em algum lugar, talvez na rede ou na capacidade da grade de processar solicitações.

b. Para determinar o tamanho dos objetos que foram recuperados a cada hora ontem, adicione a opção de tamanho(`-s`) ao comando:

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

Esses resultados indicam que algumas recuperações muito grandes ocorreram quando o tráfego geral de recuperação estava no máximo.

c. Para ver mais detalhes, use o"ferramenta audit-explain" para revisar todas as operações do SGET durante aquela hora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Se a saída do comando grep for esperada em muitas linhas, adicione o `less` comando para mostrar o conteúdo do arquivo de log de auditoria uma página (uma tela) por vez.

5. Se você quiser determinar se as operações SPUT em buckets são mais lentas do que as operações SPUT para objetos:

a. Comece usando o `-go` opção, que agrupa mensagens para operações de objeto e bucket separadamente:

```
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
```

Os resultados mostram que as operações SPUT para buckets têm características de desempenho diferentes das operações SPUT para objetos.

b. Para determinar quais buckets têm as operações SPUT mais lentas, use o `-gb` opção, que agrupa mensagens por bucket:

```
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.ldt002                  1564563        0.011          51.569
0.361
```

c. Para determinar quais buckets têm o maior tamanho de objeto SPUT, use ambos `-gb` e o `-s` opções:

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                    count       min(B)          max(B)
average(B)
  =============                    =====     ========        ========
============
  SPUT.cho-non-versioning          71943        2.097        5000.000
21.672
  SPUT.cho-versioning              54277        2.097        5000.000
21.120
  SPUT.cho-west-region             80615        2.097         800.000
14.433
  SPUT.ldt002                    1564563        0.000         999.972
0.352
```

Formato de mensagem de auditoria

Formato de mensagem de auditoria

As mensagens de auditoria trocadas dentro do sistema StorageGRID incluem informações padrão comuns a todas as mensagens e conteúdo específico descrevendo o evento ou atividade que está sendo relatada.

Se as informações resumidas fornecidas pelo"auditoria-explicação" e"soma de auditoria" ferramentas for insuficiente, consulte esta seção para entender 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 sequência de elementos de atributo. A sequência inteira está entre colchetes(`[ ]`), e cada elemento de atributo na string tem as seguintes características:

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

Cada elemento inclui um código de atributo, um tipo de dado 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 de atributo:

- `ATTR`é um código de quatro caracteres para o atributo que está sendo relatado. Há alguns atributos que são comuns a todas as mensagens de auditoria e outros que são específicos do evento.
- `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 sempre seguem dois pontos(:`). Valores do tipo de dados CSTR são colocados entre aspas duplas " ".

Tipos de dados

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

Tipo	Descrição
UI32	Inteiro longo sem sinal (32 bits); pode armazenar os números de 0 a 4.294.967.295.
UI64	Inteiro duplo longo sem sinal (64 bits); pode armazenar os números de 0 a 18.446.744.073.709.551.615.
FC32	Constante de quatro caracteres; um valor inteiro sem sinal de 32 bits representado como quatro caracteres ASCII, como "ABCD".
iPad	Usado para endereços IP.
CSTR	Uma matriz de comprimento variável de caracteres UTF-8. Os caracteres podem ser escapados com as seguintes convenções: • A barra invertida é \\. • O retorno de carro é \r. • Aspas duplas são \". • A quebra de linha (nova linha) é \n. • Os caracteres podem ser substituídos por seus equivalentes hexadecimais (no formato \xHH, 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 de um evento do sistema.

Após a abertura `[AUDT:` contêiner que identifica a mensagem em si, o próximo conjunto de atributos fornece informações sobre o evento ou ação descrita pela mensagem de auditoria. Esses atributos são destacados no exemplo a seguir:

```
2018-12-05T08:24:45.921845 [AUDT:*\[RSLT\(FC32\):SUCS\]*
\[TIME\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025621595611246499"\]
\[SACC\(CSTR\):"conta"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsKJ
A=="\] \[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"conta"\]\[S3BK\(CSTR\):"bucket"\]
\[S3KY\(CSTR\):"objeto"\]\[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]]
```

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

Elementos comuns em mensagens de auditoria

Todas as mensagens de auditoria contêm os elementos comuns.

Código	Tipo	Descrição
ENTRE	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: 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, esse elemento indicava o horário em que o sistema de auditoria foi inicializado após o serviço ser iniciado. Este valor de tempo foi medido em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1º de janeiro de 1970). **Observação:** Este elemento está obsoleto e não aparece mais nas mensagens de auditoria.

Código	Tipo	Descrição
ASQN	UI64	Contagem de sequência: em versões anteriores, esse contador era incrementado para cada mensagem de auditoria gerada no nó da grade (ANID) e zerado na reinicialização do serviço. **Observação:** Este elemento está obsoleto e não aparece mais nas mensagens de auditoria.
ATID	UI64	ID de rastreamento: um identificador compartilhado pelo conjunto de mensagens que foram acionadas por um único evento.
ATIM	UI64	Carimbo de data/hora: hora em que o evento foi gerado e que disparou a mensagem de auditoria, medido em microssegundos desde a época do sistema operacional (00:00:00 UTC em 1º de janeiro de 1970). Observe que a maioria das ferramentas disponíveis para converter o registro de data e hora em data e hora locais são baseadas em milissegundos. Pode ser necessário arredondar ou truncar o registro de data e hora registrado. 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 sequência literal que indica o início do segmento de tempo da data. *`UUUUUU`* são microssegundos.
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 são incluídos.
MÉDIO	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 com versões anteriores no serviço AMS para processar mensagens de versões mais antigas dos serviços.
RSLT	FC32	Resultado: O resultado de um evento, processo ou transação. Se não for relevante para uma mensagem, NONE é 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 um exemplo de mensagem de auditoria 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 registrado, bem como informações sobre a própria mensagem de auditoria.

Para identificar qual evento é registrado 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. "CUSPIR" representa uma transação S3 PUT, que registra a ingestão de um objeto em um bucket.

A seguinte mensagem de auditoria também mostra o bucket 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 registro de data e hora do Tempo Universal Coordenado (UTC) no início da mensagem de auditoria. Este valor é uma versão legível 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]]
```

O ATIM registra o tempo, em microssegundos, desde o início da era UNIX. No exemplo, o valor `1405631878959669` traduz para quinta-feira, 17-jul-2014 21:17:59 UTC.

Mensagens de auditoria e o ciclo de vida do objeto

Quando as mensagens de auditoria são geradas?

Mensagens de auditoria são geradas sempre que um objeto é ingerido, recuperado ou excluído. Você pode identificar essas transações no log de auditoria localizando mensagens de auditoria específicas da API do S3.

As mensagens de auditoria são vinculadas por meio de identificadores específicos para cada protocolo.

Protocolo	Código
Vinculando operações S3	S3BK (balde), S3KY (chave) ou ambos
Vinculando operações Swift	WCON (contêiner), WOBJ (objeto) ou ambos
Vinculando operações internas	CBDID (identificador interno do objeto)

Cronometragem das mensagens de auditoria

Devido a fatores como diferenças de tempo entre nós da grade, tamanho do objeto e atrasos na rede, a ordem das mensagens de auditoria geradas pelos diferentes serviços pode variar daquela mostrada nos exemplos desta seção.

Transações de ingestão de objetos

Você pode identificar transações de ingestão de clientes no log de auditoria localizando mensagens de auditoria específicas da API do S3.

Nem todas as mensagens de auditoria geradas durante uma transação de ingestão estão listadas nas tabelas a seguir. Somente as mensagens necessárias para rastrear a transação de ingestão são incluídas.

Mensagens de auditoria de ingestão do S3

Código	Nome	Descrição	Rastro	Ver
CUSPIR	Transação S3 PUT	Uma transação de ingestão S3 PUT foi concluída com sucesso.	CBDI, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Regras de Objetos Atendidas	A política do ILM foi satisfeita para este objeto.	CBDI	"ORLM: Regras de Objeto Atendidas"

Mensagens de auditoria de ingestão rápida

Código	Nome	Descrição	Rastro	Ver
WPUT	Transação Swift PUT	Uma transação de ingestão Swift PUT foi concluída com sucesso.	CBDI, WCON, WOBJ	"WPUT: PUT rápido"
ORLM	Regras de Objetos Atendidas	A política do ILM foi satisfeita para este objeto.	CBDI	"ORLM: Regras de Objeto Atendidas"

Exemplo: ingestão de objeto S3

A série de mensagens de auditoria abaixo é um exemplo das mensagens de auditoria geradas e salvas no log de auditoria quando um cliente S3 ingere um objeto em um nó de armazenamento (serviço LDR).

Neste exemplo, a política ILM ativa inclui a regra ILM Fazer 2 Cópias.

> Nem todas as mensagens de auditoria geradas durante uma transação estão listadas no exemplo abaixo. Somente aqueles relacionados à transação de ingestão S3 (SPUT) são listados.

Este exemplo pressupõe que um bucket S3 foi criado anteriormente.

SPUT: S3 PUT

A mensagem SPUT é gerada para indicar que uma transação S3 PUT foi emitida para criar um objeto em um bucket específico.

```
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"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: Regras de Objeto Atendidas

A mensagem ORLM indica que a política ILM foi satisfeita para este objeto. A mensagem inclui o CBID do objeto e o nome da regra ILM que foi aplicada.

Para objetos replicados, o campo LOCS inclui o ID do nó LDR e o ID do volume dos locais do objeto.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Para objetos codificados por eliminação, o campo LOCS inclui o ID do perfil de codificação de eliminação e o ID do grupo de codificação de eliminação

```
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][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

O campo PATH inclui informações de bucket e chave do S3 ou informações de contêiner e objeto do Swift, dependendo de qual API foi usada.

```
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]]
```

Transações de exclusão de objetos

Você pode identificar transações de exclusão de objetos no log de auditoria localizando mensagens de auditoria específicas da API do S3.

Nem todas as mensagens de auditoria geradas durante uma transação de exclusão estão listadas nas tabelas a seguir. Somente mensagens necessárias para rastrear a transação de exclusão são incluídas.

Mensagens de auditoria de exclusão do S3

Código	Nome	Descrição	Rastro	Ver
SDEL	S3 Excluir	Solicitação feita para excluir o objeto de um bucket.	CBDI, S3KY	"SDEL: S3 EXCLUIR"

Mensagens de auditoria de exclusão rápida

Código	Nome	Descrição	Rastro	Ver
WDEL	Exclusão rápida	Solicitação feita para excluir o objeto de um contêiner, ou o contêiner.	CBDI, WOBJ	"WDEL: Swift EXCLUIR"

Exemplo: exclusão de objeto S3

Quando um cliente S3 exclui um objeto de um nó de armazenamento (serviço LDR), uma mensagem de auditoria é gerada e salva no log de auditoria.

> Nem todas as mensagens de auditoria geradas durante uma transação de exclusão estão listadas no exemplo abaixo. Somente aqueles relacionados à transação de exclusão do S3 (SDEL) são listados.

SDEL: S3 Excluir

A exclusão de objetos começa quando o cliente envia uma solicitação DeleteObject para um serviço LDR. A mensagem contém o bucket do qual o objeto deve ser excluído e a chave S3 do objeto, que é usada para identificá-lo.

```
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"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

Transações de recuperação de objetos

Você pode identificar transações de recuperação de objetos no log de auditoria localizando mensagens de auditoria específicas da API do S3.

Nem todas as mensagens de auditoria geradas durante uma transação de recuperação estão listadas nas tabelas a seguir. Somente mensagens necessárias para rastrear a transação de recuperação são incluídas.

Mensagens de auditoria de recuperação S3

Código	Nome	Descrição	Rastro	Ver
SGET	S3 GET	Solicitação feita para recuperar um objeto de um bucket.	CBDI, S3BK, S3KY	"SGET: S3 OBTER"

Mensagens de auditoria de recuperação rápida

Código	Nome	Descrição	Rastro	Ver
WGET	Rápido GET	Solicitação feita para recuperar um objeto de um contêiner.	CBDI, WCON, WOBJ	"WGET: GET rápido"

Exemplo: recuperação de objeto S3

Quando um cliente S3 recupera um objeto de um nó de armazenamento (serviço LDR), uma mensagem de auditoria é gerada e salva no log de auditoria.

Observe que nem todas as mensagens de auditoria geradas durante uma transação estão listadas no exemplo abaixo. Somente aqueles relacionados à transação de recuperação S3 (SGET) são listados.

SGET: S3 OBTER

A recuperação de objetos começa quando o cliente envia uma solicitação GetObject para um serviço LDR. A mensagem contém o bucket do qual recuperar o objeto e a chave S3 do objeto, que é usada para identificá-lo.

```
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][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Se a política do bucket permitir, um cliente poderá recuperar objetos anonimamente ou recuperar objetos de um bucket que pertence a uma conta de locatário diferente. A mensagem de auditoria contém informações sobre a conta do locatário do proprietário do bucket para que você possa rastrear essas solicitações anônimas e entre contas.

Na mensagem de exemplo a seguir, o cliente envia uma solicitação GetObject para um objeto armazenado em um bucket que não é dele. Os valores para SBAI e SBAC registram o ID e o nome da conta do locatário do proprietário do bucket, que diferem do ID e do nome da conta do locatário do cliente registrados no S3AI e no SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Exemplo: S3 Select em um objeto

Quando um cliente S3 emite uma consulta S3 Select em um objeto, mensagens de auditoria são geradas e salvas no log de auditoria.

Observe que nem todas as mensagens de auditoria geradas durante uma transação estão listadas no exemplo abaixo. Somente aqueles relacionados à transação S3 Select (SelectObjectContent) são listados.

Cada consulta resulta em duas mensagens de auditoria: uma que executa a autorização da solicitação S3 Select (o campo S3SR é definido como "select") e uma operação GET padrão subsequente que recupera os dados do armazenamento durante o processamento.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):13630097093968959 85]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Mensagens de atualização de metadados

Mensagens de auditoria são geradas quando um cliente S3 atualiza os metadados de um objeto.

Mensagens de auditoria de atualização de metadados S3

Código	Nome	Descrição	Rastro	Ver
SUPD	Metadados S3 atualizados	Gerado quando um cliente S3 atualiza os metadados de um objeto ingerido.	CBDI, S3KY, HTRH	"SUPD: Metadados S3 atualizados"

Exemplo: atualização de metadados S3

O exemplo mostra uma transação bem-sucedida para atualizar os metadados de um objeto S3 existente.

SUPD: Atualização de metadados S3

O cliente S3 faz uma solicitação (SUPD) para atualizar os metadados especificados(`x-amz-meta-\*`) para o objeto S3 (S3KY). Neste exemplo, os cabeçalhos de solicitação são incluídos no campo HTRH porque ele foi configurado como um cabeçalho de protocolo de auditoria (**CONFIGURAÇÃO** > **Monitoramento** > **Servidor de auditoria e syslog**). Ver "Configurar mensagens de auditoria e destinos de log" .

```
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]]
```

Mensagens de auditoria

Descrições de mensagens de auditoria

Descrições detalhadas das mensagens de auditoria retornadas pelo sistema estão listadas nas seções a seguir. Cada mensagem de auditoria é listada primeiro em uma tabela que agrupa mensagens relacionadas pela classe de atividade que a mensagem representa. Esses agrupamentos são úteis tanto para entender os tipos de atividades que são auditadas quanto para selecionar o tipo desejado de filtragem de mensagens de auditoria.

As mensagens de auditoria também são listadas em ordem alfabética por seus códigos de quatro caracteres. Esta lista alfabética permite que você encontre informações sobre mensagens específicas.

Os códigos de quatro caracteres usados neste capítulo são os valores ATYP encontrados nas mensagens de auditoria, conforme mostrado na seguinte mensagem de exemplo:

```
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):94457363265
00603516]]
```

Para obter informações sobre como definir níveis de mensagens de auditoria, alterar destinos de log e usar um servidor syslog externo para suas informações de auditoria, consulte"Configurar mensagens de auditoria e destinos de log"

Categorias de mensagens de auditoria

Mensagens de auditoria do sistema

As mensagens de auditoria pertencentes à categoria de auditoria do sistema são usadas para eventos relacionados ao próprio sistema de auditoria, estados de nós de grade, atividade de tarefas em todo o sistema (tarefas de grade) e operações de backup de serviço.

Código	Título e descrição da mensagem	Ver
ECMC	Fragmento de dados codificado por apagamento ausente: indica que um fragmento de dados codificado por apagamento ausente foi detectado.	"ECMC: Fragmento de dados codificado por apagamento ausente"
CEC	Fragmento de dados corrompido com codificação de eliminação: indica que um fragmento de dados corrompido com codificação de eliminação foi detectado.	"ECOC: Fragmento de dados codificados por apagamento corrompidos"
ETAF	Falha na autenticação de segurança: uma tentativa de conexão usando o Transport Layer Security (TLS) falhou.	"ETAF: Falha na autenticação de segurança"
GNRG	Registro GNDS: Um serviço atualiza ou registra informações sobre si mesmo no sistema StorageGRID .	"GNRG: Registro GNDS"
GNUR	Cancelamento de registro do GNDS: um serviço cancelou seu registro no sistema StorageGRID .	"GNUR: Cancelamento de registro do GNDS"
GTED	Tarefa de grade encerrada: o serviço CMN concluiu o processamento da tarefa de grade.	"GTED: Tarefa de grade encerrada"
GTST	Tarefa de grade iniciada: o serviço CMN começou a processar a tarefa de grade.	"GTST: Tarefa de grade iniciada"

Código	Título e descrição da mensagem	Ver
GTSU	Tarefa de grade enviada: uma tarefa de grade foi enviada ao serviço CMN.	"GTSU: Tarefa de grade enviada"
LLST	Localização perdida: esta mensagem de auditoria é gerada quando uma localização é perdida.	"LLST: Localização Perdida"
OLST	Objeto perdido: um objeto solicitado não pode ser localizado no sistema StorageGRID .	"OLST: Sistema detectou objeto perdido"
SADD	Desativar auditoria de segurança: o registro de mensagens de auditoria foi desativado.	"SADD: Desativação de auditoria de segurança"
SADE	Habilitar auditoria de segurança: o registro de mensagens de auditoria foi restaurado.	"SADE: Habilitar Auditoria de Segurança"
SVRF	Falha na verificação do Object Store: um bloco de conteúdo falhou nas verificações.	"SVRF: Falha na verificação do armazenamento de objetos"
SVRU	Object Store Verify Unknown: Dados de objeto inesperados detectados no armazenamento de objetos.	"SVRU: Verificação de armazenamento de objeto desconhecido"
SYSD	Parada do nó: um desligamento foi solicitado.	"SYSD: Parada do nó"
SISTEMA	Parada de nó: um serviço iniciou uma parada normal.	"SYST: Parada do nó"
SYSU	Início do nó: um serviço foi iniciado; a natureza do desligamento anterior é indicada na mensagem.	"SYSU: Início do nó"

Mensagens de auditoria de armazenamento de objetos

As mensagens de auditoria pertencentes à categoria de auditoria de armazenamento de objetos são usadas para eventos relacionados ao armazenamento e gerenciamento de objetos dentro do sistema StorageGRID . Isso inclui armazenamento e recuperação de objetos, transferências de nó de grade para nó de grade e verificações.

> ⓘ Os códigos de auditoria são removidos do produto e da documentação, pois os recursos são descontinuados. Se você encontrar um código de auditoria que não esteja listado aqui, verifique as versões anteriores deste tópico para versões mais antigas do SG. Por exemplo, "Mensagens de auditoria de armazenamento de objetos do StorageGRID 11.8" .

Código	Descrição	Ver
IRMÃO	Solicitação de somente leitura de bucket: um bucket entrou ou saiu do modo somente leitura.	"BROR: Solicitação de somente leitura do bucket"
CBSE	Fim do envio do objeto: a entidade de origem concluiu uma operação de transferência de dados de um nó da grade para outro.	"CBSE: Fim do envio de objeto"
CBRE	Fim do recebimento do objeto: a entidade de destino concluiu uma operação de transferência de dados de um nó da grade para outro.	"CBRE: Objeto Recebimento Final"
CGRR	Solicitação de replicação entre grades: o StorageGRID tentou uma operação de replicação entre grades para replicar objetos entre buckets em uma conexão de federação de grade.	"CGRR: Solicitação de replicação entre redes"
EBDL	Exclusão de bucket vazio: o scanner ILM excluiu um objeto em um bucket que está excluindo todos os objetos (executando uma operação de bucket vazio).	"EBDL: Exclusão de Bucket Vazio"
EBKR	Solicitação de bucket vazio: um usuário enviou uma solicitação para ativar ou desativar o bucket vazio (ou seja, para excluir objetos do bucket ou para parar de excluir objetos).	"EBKR: Solicitação de balde vazio"
SCMT	Confirmação do armazenamento de objetos: um bloco de conteúdo foi completamente armazenado e verificado e agora pode ser solicitado.	"SCMT: Solicitação de confirmação de armazenamento de objeto"
SREM	Remoção do Object Store: Um bloco de conteúdo foi excluído de um nó de grade e não pode mais ser solicitado diretamente.	"SREM: Remoção de armazenamento de objetos"

O cliente leu mensagens de auditoria

As mensagens de auditoria de leitura do cliente são registradas quando um aplicativo cliente S3 faz uma solicitação para recuperar um objeto.

Código	Descrição	Usado por	Ver
S3SL	Solicitação S3 Select: Registra uma conclusão depois que uma solicitação S3 Select é retornada ao cliente. A mensagem S3SL pode incluir detalhes da mensagem de erro e do código de erro. A solicitação pode não ter sido bem-sucedida.	Cliente S3	"S3SL: Solicitação de seleção S3"

Código	Descrição	Usado por	Ver
SGET	S3 GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um bucket. **Observação:** Se a transação operar em um sub-recurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SGET: S3 OBTER"
KARITÉ	S3 HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou bucket.	Cliente S3	"SHEA: CABEÇA S3"
WGET	Swift GET: Registra uma transação bem-sucedida para recuperar um objeto ou listar os objetos em um contêiner.	Cliente Swift	"WGET: GET rápido"
WHEA	Swift HEAD: Registra uma transação bem-sucedida para verificar a existência de um objeto ou contêiner.	Cliente Swift	"WHEA: CABEÇA Rápida"

O cliente escreve mensagens de auditoria

As mensagens de auditoria de gravação do cliente são registradas quando um aplicativo cliente S3 faz uma solicitação para criar ou modificar um objeto.

Código	Descrição	Usado por	Ver
OVWR	Substituição de objeto: registra uma transação para substituir um objeto por outro objeto.	Clientes S3 e Swift	"OVWR: Substituição de Objeto"
SDEL	S3 DELETE: Registra uma transação bem-sucedida para excluir um objeto ou bucket. **Observação:** Se a transação operar em um sub-recurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SDEL: S3 EXCLUIR"
SPOS	S3 POST: Registra uma transação bem-sucedida para restaurar um objeto do armazenamento do AWS Glacier para um pool de armazenamento em nuvem.	Cliente S3	"SPOS: POSTAGEM S3"
CUSPIR	S3 PUT: Registra uma transação bem-sucedida para criar um novo objeto ou bucket. **Observação:** Se a transação operar em um sub-recurso, a mensagem de auditoria incluirá o campo S3SR.	Cliente S3	"SPUT: S3 PUT"

Código	Descrição	Usado por	Ver
SUPD	Metadados S3 atualizados: registra uma transação bem-sucedida para atualizar os metadados de um objeto ou bucket existente.	Cliente S3	"SUPD: Metadados S3 atualizados"
WDEL	Swift DELETE: Registra uma transação bem-sucedida para excluir um objeto ou contêiner.	Cliente Swift	"WDEL: Swift EXCLUIR"
WPUT	Swift PUT: Registra uma transação bem-sucedida para criar um novo objeto ou contêiner.	Cliente Swift	"WPUT: PUT rápido"

Mensagem de auditoria de gestão

A categoria Gerenciamento registra solicitações do usuário na API de Gerenciamento.

Código	Título e descrição da mensagem	Ver
MGAU	Mensagem de auditoria da API de gerenciamento: um log de solicitações do usuário.	"MGAU: Mensagem de auditoria de gestão"

Mensagens de auditoria do ILM

As mensagens de auditoria pertencentes à categoria de auditoria ILM são usadas para eventos relacionados às operações de gerenciamento do ciclo de vida da informação (ILM).

Código	Título e descrição da mensagem	Ver
IDEL	Exclusão iniciada pelo ILM: esta mensagem de auditoria é gerada quando o ILM inicia o processo de exclusão de um objeto.	"IDEL: Exclusão iniciada pelo ILM"
LKCU	Limpeza de objetos sobrescritos. Esta mensagem de auditoria é gerada quando um objeto substituído é removido automaticamente para liberar espaço de armazenamento.	"LKCU: Limpeza de Objetos Sobrescritos"
ORLM	Regras de objeto atendidas: esta mensagem de auditoria é gerada quando os dados do objeto são armazenados conforme especificado pelas regras do ILM.	"ORLM: Regras de Objeto Atendidas"

Referência de mensagem de auditoria

BROR: Solicitação de somente leitura do bucket

O serviço LDR gera esta mensagem de auditoria quando um bucket entra ou sai do modo somente leitura. Por exemplo, um bucket entra no modo somente leitura enquanto

todos os objetos estão sendo excluídos.

Código	Campo	Descrição
BKHD	UUID do balde	O ID do bucket.
IRMÃO	Valor de solicitação somente leitura do bucket	Se o bucket está se tornando somente leitura ou está saindo do estado somente leitura (1 = somente leitura, 0 = não somente leitura).
MANOS	Motivo de somente leitura do bucket	O motivo pelo qual o bucket está se tornando somente leitura ou saindo do estado somente leitura. Por exemplo, emptyBucket.
S3AI	ID da conta do locatário S3	O ID da conta do locatário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.

CBRB: Início do recebimento do objeto

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre diferentes nós à medida que os dados são acessados, replicados e retidos. Quando a transferência de um bloco de conteúdo de um nó para outro é iniciada, esta mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo da sessão/conexão nó a nó.
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: A operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.

Código	Campo	Descrição
CTDS	Entidade de Destino	O ID do nó do destino (receptor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a primeira contagem de sequência solicitada. Se bem-sucedido, a transferência começa a partir desta contagem de sequência.
CTES	Contagem de sequência final esperada	Indica a última contagem de sequência solicitada. Se bem-sucedida, a transferência será considerada concluída quando esta contagem de sequência for recebida.
RSLT	Status de início da transferência	Status no momento em que a transferência foi iniciada: SUCS: Transferência iniciada com sucesso.

Esta mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi iniciada em um único pedaço de conteúdo, conforme identificado pelo seu Identificador de Bloco de Conteúdo. A operação solicita dados de "Contagem de sequência inicial" até "Contagem de sequência final esperada". Os nós de envio e recebimento são identificados por seus IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e, quando combinadas com mensagens de auditoria de armazenamento, para verificar contagens de réplicas.

CBRE: Objeto Recebimento Final

Quando a transferência de um bloco de conteúdo de um nó para outro é concluída, esta mensagem é emitida pela entidade de destino.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo da sessão/conexão nó a nó.
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: A operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.

Código	Campo	Descrição
CTDS	Entidade de Destino	O ID do nó do destino (receptor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a contagem de sequência na qual a transferência começou.
CTAS	Contagem real da sequência final	Indica a última contagem de sequência transferida com sucesso. Se a Contagem de Sequência Final Real for a mesma que a Contagem de Sequência Inicial e o Resultado da Transferência não for bem-sucedido, nenhum dado foi trocado.
RSLT	Resultado da transferência	O resultado da operação de transferência (da perspectiva da entidade remetente): SUCS: transferência concluída com sucesso; todas as contagens de sequência solicitadas foram enviadas. CONL: conexão perdida durante a transferência CTMO: tempo limite de conexão durante estabelecimento ou transferência UNRE: ID do nó de destino inacessível CRPT: transferência encerrada devido ao recebimento de dados corrompidos ou inválidos

Esta mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi concluída. Se o resultado da transferência for bem-sucedido, a operação transfere dados de "Contagem de sequência inicial" para "Contagem de sequência final real". Os nós de envio e recebimento são identificados por seus IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e para localizar, tabular e analisar erros. Quando combinado com mensagens de auditoria de armazenamento, também pode ser usado para verificar contagens de réplicas.

CBSB: Início do envio de objeto

Durante as operações normais do sistema, os blocos de conteúdo são continuamente transferidos entre diferentes nós à medida que os dados são acessados, replicados e retidos. Quando a transferência de um bloco de conteúdo de um nó para outro é iniciada, esta mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo da sessão/conexão nó a nó.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: A operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de Destino	O ID do nó do destino (receptor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a primeira contagem de sequência solicitada. Se bem-sucedido, a transferência começa a partir desta contagem de sequência.
CTES	Contagem de sequência final esperada	Indica a última contagem de sequência solicitada. Se bem-sucedida, a transferência será considerada concluída quando esta contagem de sequência for recebida.
RSLT	Status de início da transferência	Status no momento em que a transferência foi iniciada: SUCS: transferência iniciada com sucesso.

Esta mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi iniciada em um único pedaço de conteúdo, conforme identificado pelo seu Identificador de Bloco de Conteúdo. A operação solicita dados de "Contagem de sequência inicial" até "Contagem de sequência final esperada". Os nós de envio e recebimento são identificados por seus IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e, quando combinadas com mensagens de auditoria de armazenamento, para verificar contagens de réplicas.

CBSE: Fim do envio de objeto

Quando a transferência de um bloco de conteúdo de um nó para outro é concluída, esta mensagem é emitida pela entidade de origem.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo da sessão/conexão nó a nó.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que está sendo transferido.
CTDR	Direção de transferência	Indica se a transferência CBID foi iniciada por push ou pull: PUSH: A operação de transferência foi solicitada pela entidade remetente. PULL: A operação de transferência foi solicitada pela entidade receptora.
CTSR	Entidade de origem	O ID do nó da origem (remetente) da transferência CBID.
CTDS	Entidade de Destino	O ID do nó do destino (receptor) da transferência CBID.
CTSS	Iniciar contagem de sequência	Indica a contagem de sequência na qual a transferência começou.
CTAS	Contagem real da sequência final	Indica a última contagem de sequência transferida com sucesso. Se a Contagem de Sequência Final Real for a mesma que a Contagem de Sequência Inicial e o Resultado da Transferência não for bem-sucedido, nenhum dado foi trocado.
RSLT	Resultado da transferência	O resultado da operação de transferência (da perspectiva da entidade remetente): SUCS: Transferência concluída com sucesso; todas as contagens de sequência solicitadas foram enviadas. CONL: conexão perdida durante a transferência CTMO: tempo limite de conexão durante estabelecimento ou transferência UNRE: ID do nó de destino inacessível CRPT: transferência encerrada devido ao recebimento de dados corrompidos ou inválidos

Esta mensagem de auditoria significa que uma operação de transferência de dados de nó para nó foi concluída. Se o resultado da transferência for bem-sucedido, a operação transfere dados de "Contagem de sequência inicial" para "Contagem de sequência final real". Os nós de envio e recebimento são identificados por seus IDs de nó. Essas informações podem ser usadas para rastrear o fluxo de dados do sistema e para localizar, tabular e analisar erros. Quando combinado com mensagens de auditoria de armazenamento, também pode ser usado para verificar contagens de réplicas.

CGRR: Solicitação de replicação entre redes

Esta mensagem é gerada quando o StorageGRID tenta uma operação de replicação entre grades para replicar objetos entre buckets em uma conexão de federação de grade.

Código	Campo	Descrição
CSIZ	Tamanho do objeto	O tamanho do objeto em bytes. O atributo CSIZ foi introduzido no StorageGRID 11.8. Como resultado, as solicitações de replicação entre grades abrangendo uma atualização do StorageGRID 11.7 para 11.8 podem ter um tamanho total de objeto impreciso.
S3AI	ID da conta do locatário S3	O ID da conta do locatário que possui o bucket do qual o objeto está sendo replicado.
GFID	ID de conexão da federação de grade	O ID da conexão de federação de grade que está sendo usada para replicação entre grades.
OPER	Operação CGR	O tipo de operação de replicação entre grades que foi tentada: • 0 = Replicar objeto • 1 = Replicar objeto multiparte • 2 = Replicar marcador de exclusão
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket.
VSID	ID da versão	O ID da versão específica de um objeto que estava sendo replicado.
RSLT	Código de resultado	Retorna erro bem-sucedido (SUCS) ou erro geral (GERR).

EBDL: Exclusão de Bucket Vazio

O scanner ILM excluiu um objeto em um bucket que está excluindo todos os objetos (executando uma operação de bucket vazio).

Código	Campo	Descrição
CSIZ	Tamanho do objeto	O tamanho do objeto em bytes.
CAMINHO	Balde/Chave S3	O nome do bucket S3 e o nome da chave S3.

Código	Campo	Descrição
SEGC	UUID do contêiner	UUID do contêiner para o objeto segmentado. Este valor só estará disponível se o objeto for segmentado.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
RSLT	Resultado da operação de exclusão	O resultado de um evento, processo ou transação. Se não for relevante para uma mensagem, NONE é usado em vez de SUCS para que a mensagem não seja filtrada acidentalmente.

EBKR: Solicitação de balde vazio

Esta mensagem indica que um usuário enviou uma solicitação para ativar ou desativar o bucket vazio (ou seja, para excluir objetos do bucket ou para parar de excluir objetos).

Código	Campo	Descrição
CONSTRUIR	UUID do balde	O ID do bucket.
EBJS	Configuração JSON do Bucket Vazio	Contém o JSON que representa a configuração atual do Empty Bucket.
S3AI	ID da conta do locatário S3	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.

ECMC: Fragmento de dados codificado por apagamento ausente

Esta mensagem de auditoria indica que o sistema detectou um fragmento de dados codificado para eliminação ausente.

Código	Campo	Descrição
VCMC	ID do VCS	O nome do VCS que contém o pedaço faltante.
MCID	ID do pedaço	O identificador do fragmento codificado por apagamento ausente.
RSLT	Resultado	Este campo tem o valor 'NENHUM'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem específica. 'NONE' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

ECOC: Fragmento de dados codificados por apagamento corrompidos

Esta mensagem de auditoria indica que o sistema detectou um fragmento de dados corrompido com código de eliminação.

Código	Campo	Descrição
VCCO	ID do VCS	O nome do VCS que contém o pedaço corrompido.
VLID	ID do volume	O volume RangeDB que contém o fragmento corrompido com código de eliminação.
CCID	ID do pedaço	O identificador do fragmento corrompido codificado por apagamento.
RSLT	Resultado	Este campo tem o valor 'NENHUM'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem específica. 'NONE' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

ETAF: Falha na autenticação de segurança

Esta mensagem é gerada quando uma tentativa de conexão usando o Transport Layer Security (TLS) falha.

Código	Campo	Descrição
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP na qual a autenticação falhou.
RUID	Identidade do usuário	Um identificador dependente de serviço que representa a identidade do usuário remoto.

Código	Campo	Descrição
RSLT	Código de Razão	O motivo da falha: SCNI: Falha no estabelecimento da conexão segura. CERM: O certificado estava faltando. CERT: O certificado era inválido. CERE: O certificado expirou. CERR: O certificado foi revogado. CSGN: A assinatura do certificado era inválida. CSGU: O signatário do certificado era desconhecido. UCRM: As credenciais do usuário estavam faltando. UCRI: As credenciais do usuário eram inválidas. UCRU: Credenciais de usuário não foram permitidas. TOUT: Tempo limite de autenticação esgotado.

Quando uma conexão é estabelecida com um serviço seguro que usa TLS, as credenciais da entidade remota são verificadas usando o perfil TLS e lógica adicional incorporada ao serviço. Se essa autenticação falhar devido a certificados ou credenciais inválidos, inesperados ou não permitidos, uma mensagem de auditoria será registrada. Isso permite consultas sobre tentativas de acesso não autorizado e outros problemas de conexão relacionados à segurança.

A mensagem pode resultar de uma entidade remota com configuração incorreta ou de tentativas de apresentar credenciais inválidas ou não permitidas ao sistema. Esta mensagem de auditoria deve ser monitorada para detectar tentativas de obter acesso não autorizado ao sistema.

GNRG: Registro GNDS

O serviço CMN gera esta mensagem de auditoria quando um serviço atualiza ou registra informações sobre si mesmo no sistema StorageGRID .

Código	Campo	Descrição
RSLT	Resultado	O resultado da solicitação de atualização: • SUCS: Bem-sucedido • SUNV: Serviço indisponível • GERR: Outra falha
GNID	ID do nó	O ID do nó do serviço que iniciou a solicitação de atualização.

Código	Campo	Descrição
GNTP	Tipo de dispositivo	O tipo de dispositivo do nó da grade (por exemplo, BLDR para um serviço LDR).
GNDV	Versão do modelo do dispositivo	A sequência de caracteres que identifica a versão do modelo do dispositivo do nó da grade no pacote DMDL.
GNGP	Grupo	O grupo ao qual o nó da grade pertence (no contexto de custos de link e classificação de consulta de serviço).
GNIA	Endereço IP	Endereço IP do nó da grade.

Esta mensagem é gerada sempre que um nó de grade atualiza sua entrada no Pacote de Nós de Grade.

GNUR: Cancelamento de registro do GNDS

O serviço CMN gera esta mensagem de auditoria quando um serviço possui informações não registradas sobre si mesmo no sistema StorageGRID .

Código	Campo	Descrição
RSLT	Resultado	O resultado da solicitação de atualização: • SUCS: Bem-sucedido • SUNV: Serviço indisponível • GERR: Outra falha
GNID	ID do nó	O ID do nó do serviço que iniciou a solicitação de atualização.

GTED: Tarefa de grade encerrada

Esta mensagem de auditoria indica que o serviço CMN concluiu o processamento da tarefa de grade especificada e moveu a tarefa para a tabela Histórica. Se o resultado for SUCS, ABRT ou ROLF, haverá uma mensagem de auditoria correspondente de Tarefa de grade iniciada. Os outros resultados indicam que o processamento desta tarefa de grade nunca foi iniciado.

Código	Campo	Descrição
TSID	ID da tarefa	Este campo identifica exclusivamente uma tarefa de grade gerada e permite que a tarefa de grade seja gerenciada ao longo de seu ciclo de vida. **Observação:** O ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, nesse caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria Enviadas, Iniciadas e Encerradas.
RSLT	Resultado	O resultado final do status da tarefa de grade: • SUCS: A tarefa da grade foi concluída com sucesso. • ABRT: A tarefa da grade foi encerrada sem erro de reversão. • ROLF: A tarefa da grade foi encerrada e não foi possível concluir o processo de reversão. • CANC: A tarefa da grade foi cancelada pelo usuário antes de ser iniciada. • EXPR: A tarefa de grade expirou antes de ser iniciada. • IVLD: A tarefa de grade era inválida. • AUTH: A tarefa de grade não foi autorizada. • DUPL: A tarefa de grade foi rejeitada como duplicada.

GTST: Tarefa de grade iniciada

Esta mensagem de auditoria indica que o serviço CMN começou a processar a tarefa de grade especificada. A mensagem de auditoria segue imediatamente a mensagem Grid Task Submitted para tarefas de grade iniciadas pelo serviço interno Grid Task Submission e selecionadas para ativação automática. Para tarefas de grade enviadas para a tabela Pendente, esta mensagem é gerada quando o usuário inicia a tarefa de grade.

Código	Campo	Descrição
TSID	ID da tarefa	Este campo identifica exclusivamente uma tarefa de grade gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida. **Observação:** O ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, nesse caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria Enviadas, Iniciadas e Encerradas.

Código	Campo	Descrição
RSLT	Resultado	O resultado. Este campo tem apenas um valor: • SUCS: A tarefa de grade foi iniciada com sucesso.

GTSU: Tarefa de grade enviada

Esta mensagem de auditoria indica que uma tarefa de grade foi enviada ao serviço CMN.

Código	Campo	Descrição
TSID	ID da tarefa	Identifica exclusivamente uma tarefa de grade gerada e permite que a tarefa seja gerenciada ao longo de seu ciclo de vida. **Observação:** O ID da tarefa é atribuído no momento em que uma tarefa de grade é gerada, não no momento em que ela é enviada. É possível que uma determinada tarefa de grade seja enviada várias vezes e, nesse caso, o campo ID da tarefa não é suficiente para vincular exclusivamente as mensagens de auditoria Enviadas, Iniciadas e Encerradas.
TTYP	Tipo de tarefa	O tipo de tarefa de grade.
TVER	Versão da tarefa	Um número que indica a versão da tarefa de grade.
TDSC	Descrição da tarefa	Uma descrição legível da tarefa da grade.
IVA	Válido após o carimbo de data/hora	O primeiro momento (UINT64 microssegundos a partir de 1º de janeiro de 1970 - horário UNIX) em que a tarefa de grade é válida.
VBTS	Válido antes do carimbo de data/hora	O horário mais recente (UINT64 microssegundos a partir de 1º de janeiro de 1970 - horário UNIX) em que a tarefa de grade é válida.
TSRC	Fonte	A fonte da tarefa: • TXTB: A tarefa de grade foi enviada por meio do sistema StorageGRID como um bloco de texto assinado. • GRADE: A tarefa de grade foi enviada por meio do Serviço de Envio de Tarefas de Grade interno.
ACTV	Tipo de ativação	O tipo de ativação: • AUTO: A tarefa de grade foi enviada para ativação automática. • PEND: A tarefa da grade foi enviada para a tabela pendente. Esta é a única possibilidade para a fonte TXTB.

Código	Campo	Descrição
RSLT	Resultado	O resultado da submissão: • SUCS: A tarefa de grade foi enviada com sucesso. • FALHA: A tarefa foi movida diretamente para a tabela histórica.

IDEL: Exclusão iniciada pelo ILM

Esta mensagem é gerada quando o ILM inicia o processo de exclusão de um objeto.

A mensagem IDEL é gerada em qualquer uma destas situações:

- **Para objetos em buckets S3 compatíveis**: Esta mensagem é gerada quando o ILM inicia o processo de exclusão automática de um objeto porque seu período de retenção expirou (assumindo que a configuração de exclusão automática esteja ativada e a retenção legal esteja desativada).
- **Para objetos em buckets S3 não compatíveis**. Esta mensagem é gerada quando o ILM inicia o processo de exclusão de um objeto porque nenhuma instrução de posicionamento nas políticas ativas do ILM se aplica atualmente ao objeto.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O CBDID do objeto.
APLV	Conformidade: Exclusão automática	Somente para objetos em buckets S3 compatíveis. 0 (falso) ou 1 (verdadeiro), indicando se um objeto compatível deve ser excluído automaticamente quando seu período de retenção terminar, a menos que o bucket esteja sob retenção legal.
CMPL	Conformidade: retenção legal	Somente para objetos em buckets S3 compatíveis. 0 (falso) ou 1 (verdadeiro), indicando se o bucket está atualmente sob retenção legal.
CMPR	Conformidade: Período de retenção	Somente para objetos em buckets S3 compatíveis. A duração do período de retenção do objeto em minutos.
CTME	Conformidade: Tempo de ingestão	Somente para objetos em buckets S3 compatíveis. Tempo de ingestão do objeto. Você pode adicionar o período de retenção em minutos a esse valor para determinar quando o objeto pode ser excluído do bucket.
DMRK	Excluir ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket versionado. Operações em buckets não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.

Código	Campo	Descrição
LOCS	Locais	O local de armazenamento de dados de objetos dentro do sistema StorageGRID . O valor para LOCS é "" se o objeto não tiver localizações (por exemplo, ele foi excluído). CLEC: para objetos codificados por eliminação, o ID do perfil de codificação por eliminação e o ID do grupo de codificação por eliminação que são aplicados aos dados do objeto. CLDI: para objetos replicados, o ID do nó LDR e o ID do volume do local do objeto. CLNL: ID do nó ARC da localização do objeto se os dados do objeto estiverem arquivados.
CAMINHO	Balde/Chave S3	O nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	O resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.
REGRA	Etiqueta de regras	• Se um objeto em um bucket S3 compatível estiver sendo excluído automaticamente porque seu período de retenção expirou, este campo ficará em branco. • Se o objeto estiver sendo excluído porque não há mais instruções de posicionamento que se apliquem atualmente ao objeto, este campo mostrará o rótulo legível da última regra do ILM aplicada ao objeto.
SGRP	Site (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o site onde o objeto foi ingerido.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi excluído. Operações em buckets e objetos em buckets não versionados não incluem este campo.

LKCU: Limpeza de Objetos Sobrescritos

Esta mensagem é gerada quando o StorageGRID remove um objeto substituído que anteriormente exigia limpeza para liberar espaço de armazenamento. Um objeto é substituído quando um cliente S3 grava um objeto em um caminho que já contém um objeto. O processo de remoção ocorre automaticamente e em segundo plano.

Código	Campo	Descrição
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.
LTYP	Tipo de limpeza	*Somente para uso interno.*
LUID	UUID do objeto removido	O identificador do objeto que foi removido.
CAMINHO	Balde/Chave S3	O nome do bucket S3 e o nome da chave S3.
SEGC	UUID do contêiner	UUID do contêiner para o objeto segmentado. Este valor só estará disponível se o objeto for segmentado.
UUID	Identificador Universalmente Único	O identificador do objeto que ainda existe. Este valor só estará disponível se o objeto não tiver sido excluído.

LKDM: Limpeza de Objetos Vazados

Esta mensagem é gerada quando um pedaço vazado é limpo ou excluído. Um pedaço pode ser parte de um objeto replicado ou de um objeto codificado para eliminação.

Código	Campo	Descrição
CLOC	Localização do pedaço	O caminho do arquivo do pedaço vazado que foi excluído.

CTYP	Tipo de pedaço	Tipo de pedaço:
		`ec: Erasure-coded object chunk`
		`repl: Replicated object chunk`

Código	Campo	Descrição

LTYP	Tipo de vazamento	Os cinco tipos de vazamentos que podem ser detectados:
		
		`object_leaked: Object doesn’t exist in the grid`
		
		`location_leaked: Object exists in the grid, but found location doesn’t belong to object`
		
		`mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out`
		
		`segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn’t contain this segment`
		
		`no_parent: Container object is deleted, but object segment was left out and not deleted`

CTIM	Tempo de criação do bloco	Horário em que o pedaço vazado foi criado.
UUID	Identificador Universalmente Único	O identificador do objeto ao qual o pedaço pertence.
CBDI	Identificador de bloco de conteúdo	CBID do objeto ao qual o pedaço vazado pertence.
CSIZ	Tamanho do conteúdo	O tamanho do pedaço em bytes.

LLST: Localização Perdida

Esta mensagem é gerada sempre que um local para uma cópia de objeto (replicada ou codificada para eliminação) não pode ser encontrado.

Código	Campo	Descrição
CBIL	CBDI	O CBDI afetado.
ECPR	Perfil de codificação de apagamento	Para dados de objetos codificados por eliminação. O ID do perfil de codificação de eliminação usado.

Código	Campo	Descrição
LTYP	Tipo de localização	CLDI (Online): Para dados de objetos replicados CLEC (Online): Para dados de objetos codificados por apagamento CLNL (Nearline): Para dados de objetos replicados arquivados
NOID	ID do nó de origem	O ID do nó no qual os locais foram perdidos.
PCLD	Caminho para o objeto replicado	O caminho completo para o local do disco dos dados do objeto perdido. Retornado somente quando LTYP tem um valor de CLDI (ou seja, para objetos replicados). Assume a forma `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Resultado	Sempre NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NONE é usado em vez de SUCS para que esta mensagem não seja filtrada.
TSRC	Fonte de disparo	USUÁRIO: Acionado pelo usuário SYST: Sistema acionado
UUID	ID universalmente exclusivo	O identificador do objeto afetado no sistema StorageGRID .

MGAU: Mensagem de auditoria de gestão

A categoria Gerenciamento registra solicitações do usuário na API de Gerenciamento. Cada solicitação HTTP que não é uma solicitação GET ou HEAD para um URI de API válido registra uma resposta contendo o nome de usuário, IP e tipo de solicitação para a API. URIs de API inválidos (como /api/v3-authorize) e solicitações inválidas para URIs de API válidos não são registrados.

Código	Campo	Descrição
MDIP	Endereço IP de destino	O endereço IP do servidor (destino).
MDNA	Nome de domínio	O nome do domínio do host.
MPAT	Solicitar PATH	O caminho da solicitação.

Código	Campo	Descrição
MPQP	Parâmetros de consulta de solicitação	Os parâmetros de consulta para a solicitação.
MRBD	Corpo da solicitação	O conteúdo do corpo da solicitação. Embora o corpo da resposta seja registrado por padrão, o corpo da solicitação é registrado em certos casos quando o corpo da resposta está vazio. Como as seguintes informações não estão disponíveis no corpo da resposta, elas são obtidas do corpo da solicitação para os seguintes métodos POST: • Nome de usuário e ID da conta em **POST autorizar** • Nova configuração de sub-redes em **POST /grid/grid-networks/update** • Novos servidores NTP em **POST /grid/ntp-servers/update** • IDs de servidores desativados em **POST /grid/servers/decommission** **Observação:** Informações confidenciais são excluídas (por exemplo, uma chave de acesso S3) ou mascaradas com asteriscos (por exemplo, uma senha).
MRMD	Método de solicitação	O método de solicitação HTTP: • PUBLICAR • COLOCAR • EXCLUIR • CORREÇÃO
MRSC	Código de resposta	O código de resposta.
MRSP	Corpo de resposta	O conteúdo da resposta (o corpo da resposta) é registrado por padrão. **Observação:** Informações confidenciais são excluídas (por exemplo, uma chave de acesso S3) ou mascaradas com asteriscos (por exemplo, uma senha).
MSIP	Endereço IP de origem	O endereço IP do cliente (origem).
MUUN	URN do usuário	O URN (nome uniforme do recurso) do usuário que enviou a solicitação.
RSLT	Resultado	Retorna sucesso (SUCS) ou o erro relatado pelo backend.

OLST: Sistema detectou objeto perdido

Esta mensagem é gerada quando o serviço DDS não consegue localizar nenhuma cópia de um objeto no sistema StorageGRID .

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O CBDID do objeto perdido.
NOID	ID do nó	Se disponível, a última localização direta ou próxima conhecida do objeto perdido. É possível ter apenas o ID do nó sem um ID do volume se as informações do volume não estiverem disponíveis.
CAMINHO	Balde/Chave S3	Se disponível, o nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NONE é usado em vez de SUCS para que esta mensagem não seja filtrada.
UUID	ID universalmente exclusivo	O identificador do objeto perdido dentro do sistema StorageGRID .
VOLI	ID do volume	Se disponível, o ID do volume do nó de armazenamento para o último local conhecido do objeto perdido.

ORLM: Regras de Objeto Atendidas

Esta mensagem é gerada quando o objeto é armazenado e copiado com sucesso, conforme especificado pelas regras do ILM.

A mensagem ORLM não é gerada quando um objeto é armazenado com sucesso pela regra padrão Fazer 2 Cópias se outra regra na política usar o filtro avançado Tamanho do Objeto.

Código	Campo	Descrição
CONSTRUIR	Cabeçalho de balde	Campo ID do bucket. Usado para operações internas. Aparece somente se STAT for PRGD.
CBDI	Identificador de bloco de conteúdo	O CBDID do objeto.
CSIZ	Tamanho do conteúdo	O tamanho do objeto em bytes.

Código	Campo	Descrição
LOCS	Locais	O local de armazenamento de dados de objetos dentro do sistema StorageGRID . O valor para LOCS é "" se o objeto não tiver localizações (por exemplo, ele foi excluído). CLEC: para objetos codificados por eliminação, o ID do perfil de codificação por eliminação e o ID do grupo de codificação por eliminação que são aplicados aos dados do objeto. CLDI: para objetos replicados, o ID do nó LDR e o ID do volume do local do objeto. CLNL: ID do nó ARC da localização do objeto se os dados do objeto estiverem arquivados.
CAMINHO	Balde/Chave S3	O nome do bucket S3 e o nome da chave S3.
RSLT	Resultado	O resultado da operação ILM. SUCS: A operação ILM foi bem-sucedida.
REGRA	Etiqueta de regras	O rótulo legível dado à regra ILM aplicada a este objeto.
SEGC	UUID do contêiner	UUID do contêiner para o objeto segmentado. Este valor só estará disponível se o objeto for segmentado.
SGCB	CBDID do contêiner	CBID do contêiner para o objeto segmentado. Este valor está disponível somente para objetos segmentados e multipartes.
ESTATÍSTICA	Status	O status da operação do ILM. CONCLUÍDO: As operações do ILM contra o objeto foram concluídas. DFER: O objeto foi marcado para futura reavaliação do ILM. PRGD: O objeto foi excluído do sistema StorageGRID . NLOC: Os dados do objeto não podem mais ser encontrados no sistema StorageGRID . Esse status pode indicar que todas as cópias dos dados do objeto estão ausentes ou danificadas.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão de um novo objeto criado em um bucket versionado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

A mensagem de auditoria ORLM pode ser emitida mais de uma vez para um único objeto. Por exemplo, ele é emitido sempre que ocorre um dos seguintes eventos:

- As regras do ILM para o objeto são satisfeitas para sempre.
- As regras do ILM para o objeto são satisfeitas para esta época.
- As regras do ILM excluíram o objeto.
- O processo de verificação em segundo plano detecta que uma cópia dos dados do objeto replicado está corrompida. O sistema StorageGRID executa uma avaliação do ILM para substituir o objeto corrompido.

Informações relacionadas

- "Transações de ingestão de objetos"
- "Transações de exclusão de objetos"

OVWR: Substituição de Objeto

Esta mensagem é gerada quando uma operação externa (solicitada pelo cliente) faz com que um objeto seja substituído por outro objeto.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo (novo)	O CBDID para o novo objeto.
CSIZ	Tamanho do objeto anterior	O tamanho, em bytes, do objeto que está sendo substituído.
TOCB	Identificador de bloco de conteúdo (anterior)	O CBDID do objeto anterior.
UUID	ID universalmente exclusivo (novo)	O identificador do novo objeto dentro do sistema StorageGRID .
OUID	ID universalmente exclusivo (anterior)	O identificador do objeto anterior dentro do sistema StorageGRID .
CAMINHO	Caminho do objeto S3	O caminho do objeto S3 usado para o objeto anterior e o novo
RSLT	Código de resultado	Resultado da transação de substituição de objeto. O resultado é sempre: SUCS: Bem-sucedido

Código	Campo	Descrição
SGRP	Site (Grupo)	Se presente, o objeto substituído foi excluído no site especificado, que não é o site onde o objeto substituído foi ingerido.

S3SL: Solicitação de seleção S3

Esta mensagem registra uma conclusão após uma solicitação S3 Select ter sido retornada ao cliente. A mensagem S3SL pode incluir detalhes da mensagem de erro e do código de erro. A solicitação pode não ter sido bem-sucedida.

Código	Campo	Descrição
BYSC	Bytes escaneados	Número de bytes escaneados (recebidos) dos nós de armazenamento. BYSC e BYPR provavelmente serão diferentes se o objeto for compactado. Se o objeto for compactado, BYSC terá a contagem de bytes compactados e BYPR serão os bytes após a descompactação.
BYPR	Bytes processados	Número de bytes processados. Indica quantos bytes de "Bytes escaneados" foram realmente processados ou acionados por um trabalho S3 Select.
BYRT	Bytes retornados	Número de bytes que um trabalho S3 Select retornou ao cliente.
REPR	Registros processados	Número de registros ou linhas que um trabalho S3 Select recebeu dos nós de armazenamento.
RERT	Registros Retornados	Número de registros ou linhas que um trabalho do S3 Select retornou ao cliente.
JOFI	Trabalho concluído	Indica se o trabalho S3 Select concluiu o processamento ou não. Se isso for falso, o trabalho não foi concluído e os campos de erro provavelmente conterão dados. O cliente pode ter recebido resultados parciais ou nenhum resultado.
REID	ID da solicitação	Identificador para a solicitação S3 Select.
EXTM	Tempo de execução	O tempo, em segundos, que levou para o S3 Select Job ser concluído.
ERMG	Mensagem de erro	Mensagem de erro gerada pelo trabalho S3 Select.
ERTY	Tipo de erro	Tipo de erro gerado pelo trabalho S3 Select.
ERST	Rastreamento de pilha de erros	Rastreamento de pilha de erros gerado pelo trabalho S3 Select.

Código	Campo	Descrição
S3BK	Balde S3	O nome do bucket S3.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 para o usuário que enviou a solicitação.
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket.

SADD: Desativação de auditoria de segurança

Esta mensagem indica que o serviço de origem (ID do nó) desativou o registro de mensagens de auditoria; as mensagens de auditoria não estão mais sendo coletadas ou entregues.

Código	Campo	Descrição
AETM	Método de ativação	O método usado para desabilitar a auditoria.
AEUN	Nome de usuário	O nome de usuário que executou o comando para desabilitar o registro de auditoria.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NONE é usado em vez de SUCS para que esta mensagem não seja filtrada.

A mensagem indica que o registro estava habilitado anteriormente, mas agora foi desabilitado. Isso normalmente é usado apenas durante ingestão em massa para melhorar o desempenho do sistema. Após a atividade em massa, a auditoria é restaurada (SADE) e a capacidade de desabilitar a auditoria é bloqueada permanentemente.

SADE: Habilitar Auditoria de Segurança

Esta mensagem indica que o serviço de origem (ID do nó) restaurou o registro de mensagens de auditoria; as mensagens de auditoria estão sendo coletadas e entregues novamente.

Código	Campo	Descrição
AETM	Método de ativação	O método usado para permitir a auditoria.
AEUN	Nome de usuário	O nome de usuário que executou o comando para habilitar o registro de auditoria.
RSLT	Resultado	Este campo tem o valor NENHUM. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. NONE é usado em vez de SUCS para que esta mensagem não seja filtrada.

A mensagem indica que o registro foi desabilitado anteriormente (SADD), mas agora foi restaurado. Isso normalmente é usado apenas durante ingestão em massa para melhorar o desempenho do sistema. Após a atividade em massa, a auditoria é restaurada e a capacidade de desabilitar a auditoria é bloqueada permanentemente.

SCMT: Confirmação do Armazenamento de Objetos

O conteúdo da grade não é disponibilizado nem reconhecido como armazenado até que tenha sido confirmado (o que significa que foi armazenado persistentemente). O conteúdo armazenado de forma persistente foi completamente gravado no disco e passou pelas verificações de integridade relacionadas. Esta mensagem é emitida quando um bloco de conteúdo é confirmado no armazenamento.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo comprometido com armazenamento permanente.
RSLT	Código de resultado	Status no momento em que o objeto foi armazenado no disco: SUCS: Objeto armazenado com sucesso.

Esta mensagem significa que um determinado bloco de conteúdo foi completamente armazenado e verificado e agora pode ser solicitado. Ele pode ser usado para rastrear o fluxo de dados dentro do sistema.

SDEL: S3 EXCLUIR

Quando um cliente S3 emite uma transação DELETE, uma solicitação é feita para remover o objeto ou bucket especificado, ou para remover um sub-recurso de bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.

Código	Campo	Descrição
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto excluído em bytes. Operações em buckets não incluem este campo.
DMRK	Excluir ID da versão do marcador	O ID da versão do marcador de exclusão criado ao excluir um objeto de um bucket versionado. Operações em buckets não incluem este campo.
GFID	ID de conexão da federação de grade	O ID de conexão da federação de grade associada a uma solicitação de exclusão de replicação entre grades. Incluído somente em logs de auditoria na grade de destino.
GFSA	ID da conta de origem da Federação de Grade	O ID da conta do locatário na grade de origem para uma solicitação de exclusão de replicação entre grades. Incluído somente em logs de auditoria na grade de destino.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). `x-amz-bypass-governance-retention`é incluído automaticamente se estiver presente na solicitação.
MTME	Última hora modificada	O registro de data e hora do Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código de resultado	Resultado da transação DELETE. O resultado é sempre: SUCS: Bem-sucedido

Código	Campo	Descrição
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
S3SR	Sub-recurso S3	O bucket ou sub-recurso do objeto que está sendo operado, se aplicável.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SGRP	Site (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o site onde o objeto foi ingerido.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para solicitações anônimas.

Código	Campo	Descrição
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUDM	Identificador universalmente exclusivo para um marcador de exclusão	O identificador de um marcador de exclusão. As mensagens do log de auditoria especificam UUDM ou UUID, onde UUDM indica um marcador de exclusão criado como resultado de uma solicitação de exclusão de objeto, e UUID indica um objeto.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi excluído. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SGET: S3 OBTER

Quando um cliente S3 emite uma transação GET, uma solicitação é feita para recuperar um objeto ou listar os objetos em um bucket, ou para remover um sub-recurso de bucket/objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em buckets não incluem este campo.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
LIDADE	ListObjectsV2	Uma resposta no formato *v2* foi solicitada. Para mais detalhes, veja "AWS ListObjectsV2" . Somente para operações de bucket GET.
NCHD	Número de filhos	Inclui chaves e prefixos comuns. Somente para operações de bucket GET.
ALCANCE	Leitura de intervalo	Somente para operações de leitura de intervalo. Indica o intervalo de bytes que foi lido por esta solicitação. O valor após a barra (/) mostra o tamanho do objeto inteiro.
RSLT	Código de resultado	Resultado da transação GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
S3SR	Sub-recurso S3	O bucket ou sub-recurso do objeto que está sendo operado, se aplicável.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.

Código	Campo	Descrição
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
TRNC	Truncado ou Não Truncado	Defina como falso se todos os resultados foram retornados. Defina como verdadeiro se houver mais resultados disponíveis para retornar. Somente para operações de bucket GET.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SHEA: CABEÇA S3

Quando um cliente S3 emite uma transação HEAD, uma solicitação é feita para verificar a existência de um objeto ou bucket e recuperar os metadados sobre um objeto. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto verificado em bytes. Operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
RSLT	Código de resultado	Resultado da transação GET. O resultado é sempre: SUCS: Bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.

Código	Campo	Descrição
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SPOS: POSTAGEM S3

Quando um cliente S3 emite uma solicitação de objeto POST, esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0.

Código	Campo	Descrição
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). (Não esperado para SPOS).
RSLT	Código de resultado	Resultado da solicitação RestoreObject. O resultado é sempre: SUCS: Bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
S3SR	Sub-recurso S3	O bucket ou sub-recurso do objeto que está sendo operado, se aplicável. Defina como "selecionar" para uma operação S3 Select.

Código	Campo	Descrição
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SRCF	Configuração de sub-recursos	Restaurar informações.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto que foi solicitado. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SPUT: S3 PUT

Quando um cliente S3 emite uma transação PUT, uma solicitação é feita para criar um novo objeto ou bucket, ou para remover um sub-recurso de bucket/objeto. Esta

mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.
CMPS	Configurações de conformidade	As configurações de conformidade usadas ao criar o bucket, se presentes na solicitação (truncadas para os primeiros 1024 caracteres).
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em buckets não incluem este campo.
GFID	ID de conexão da federação de grade	O ID de conexão da federação de grade associada a uma solicitação PUT de replicação entre grades. Incluído somente em logs de auditoria na grade de destino.
GFSA	ID da conta de origem da Federação de Grade	O ID da conta do locatário na grade de origem para uma solicitação PUT de replicação entre grades. Incluído somente em logs de auditoria na grade de destino.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `` `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). `` `x-amz-bypass-governance-retention`é incluído automaticamente se estiver presente na solicitação.
LKEN	Bloqueio de objeto habilitado	Valor do cabeçalho da solicitação `x-amz-bucket-object-lock-enabled` , se presente na solicitação.

Código	Campo	Descrição
LKLH	Bloqueio de objeto - retenção legal	Valor do cabeçalho da solicitação `x-amz-object-lock-legal-hold` , se presente na solicitação PutObject.
LKMD	Modo de retenção de bloqueio de objeto	Valor do cabeçalho da solicitação `x-amz-object-lock-mode` , se presente na solicitação PutObject.
LKRU	Bloqueio de objeto reter até a data	Valor do cabeçalho da solicitação `x-amz-object-lock-retain-until-date` , se presente na solicitação PutObject. Os valores são limitados a 100 anos a partir da data em que o objeto foi ingerido.
MTME	Última hora modificada	O registro de data e hora do Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código de resultado	Resultado da transação PUT. O resultado é sempre: SUCS: Bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
S3SR	Sub-recurso S3	O bucket ou sub-recurso do objeto que está sendo operado, se aplicável.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.

Código	Campo	Descrição
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SRCF	Configuração de sub-recursos	A nova configuração de sub-recursos (truncada para os primeiros 1024 caracteres).
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
ULID	ID de upload	Incluído somente em mensagens SPUT para operações CompleteMultipartUpload. Indica que todas as peças foram carregadas e montadas.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão de um novo objeto criado em um bucket versionado. Operações em buckets e objetos em buckets não versionados não incluem este campo.
VSST	Estado de versão	O novo estado de controle de versão de um bucket. Dois estados são usados: "habilitado" ou "suspenso". Operações em objetos não incluem este campo.

SREM: Remoção de armazenamento de objetos

Esta mensagem é emitida quando o conteúdo é removido do armazenamento persistente e não está mais acessível por meio de APIs regulares.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo excluído do armazenamento permanente.
RSLT	Código de resultado	Indica o resultado das operações de remoção de conteúdo. O único valor definido é: SUCS: Conteúdo removido do armazenamento persistente

Esta mensagem de auditoria significa que um determinado bloco de conteúdo foi excluído de um nó e não pode mais ser solicitado diretamente. A mensagem pode ser usada para rastrear o fluxo de conteúdo excluído dentro do sistema.

SUPD: Metadados S3 atualizados

Esta mensagem é gerada pela API S3 quando um cliente S3 atualiza os metadados de um objeto ingerido. A mensagem é emitida pelo servidor se a atualização de metadados for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em buckets não incluem este campo.
CNCH	Cabeçalho de Controle de Consistência	O valor do cabeçalho de solicitação HTTP Consistency-Control, se presente na solicitação, ao atualizar as configurações de conformidade de um bucket.
CNID	Identificador de conexão	O identificador exclusivo do sistema para a conexão TCP/IP.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em buckets não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).

Código	Campo	Descrição
RSLT	Código de resultado	Resultado da transação GET. O resultado é sempre: SUCS: bem-sucedido
S3AI	ID da conta do locatário S3 (remetente da solicitação)	O ID da conta do locatário do usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3AK	ID da chave de acesso S3 (remetente da solicitação)	O ID da chave de acesso S3 com hash para o usuário que enviou a solicitação. Um valor vazio indica acesso anônimo.
S3BK	Balde S3	O nome do bucket S3.
S3KY	Chave S3	O nome da chave S3, sem incluir o nome do bucket. Operações em buckets não incluem este campo.
SACC	Nome da conta do locatário S3 (remetente da solicitação)	O nome da conta do locatário do usuário que enviou a solicitação. Vazio para solicitações anônimas.
SAIP	Endereço IP (remetente da solicitação)	O endereço IP do aplicativo cliente que fez a solicitação.
SBAC	Nome da conta do locatário S3 (proprietário do bucket)	O nome da conta do locatário do proprietário do bucket. Usado para identificar acesso anônimo ou entre contas.
SBAI	ID da conta do locatário S3 (proprietário do bucket)	O ID da conta do locatário do proprietário do bucket de destino. Usado para identificar acesso anônimo ou entre contas.
SUSR	URN do usuário S3 (remetente da solicitação)	O ID da conta do locatário e o nome de usuário do usuário que faz a solicitação. O usuário pode ser um usuário local ou um usuário LDAP. Por exemplo: `urn:sgws:identity::03393893651506583485:root` Vazio para solicitações anônimas.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.

Código	Campo	Descrição
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
VSID	ID da versão	O ID da versão específica de um objeto cujos metadados foram atualizados. Operações em buckets e objetos em buckets não versionados não incluem este campo.

SVRF: Falha na verificação do armazenamento de objetos

Esta mensagem é emitida sempre que um bloco de conteúdo falha no processo de verificação. Cada vez que dados de objetos replicados são lidos ou gravados no disco, várias verificações e verificações de integridade são realizadas para garantir que os dados enviados ao usuário solicitante sejam idênticos aos dados originalmente inseridos no sistema. Se alguma dessas verificações falhar, o sistema colocará automaticamente em quarentena os dados corrompidos do objeto replicado para impedir que sejam recuperados novamente.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo que falhou na verificação.
RSLT	Código de resultado	Tipo de falha de verificação: CRCF: Falha na verificação de redundância cíclica (CRC). HMAC: Falha na verificação do código de autenticação de mensagem baseado em hash (HMAC). EHSH: Hash de conteúdo criptografado inesperado. PHSH: Hash de conteúdo original inesperado. SEQC: Sequência de dados incorreta no disco. PERR: Estrutura inválida do arquivo de disco. DERR: Erro de disco. FNAM: Nome de arquivo incorreto.

Esta mensagem deve ser monitorada de perto. Falhas na verificação de conteúdo podem indicar falhas iminentes de hardware.

Para determinar qual operação acionou a mensagem, consulte o valor do campo AMID (ID do módulo). Por exemplo, um valor SVFY indica que a mensagem foi gerada pelo módulo Storage Verifier, ou seja, verificação em segundo plano, e STOR indica que a mensagem foi acionada pela recuperação de conteúdo.

SVRU: Verificação de armazenamento de objeto desconhecido

O componente de armazenamento do serviço LDR verifica continuamente todas as cópias de dados de objetos replicados no armazenamento de objetos. Esta mensagem é emitida quando uma cópia desconhecida ou inesperada de dados de objetos replicados é detectada no armazenamento de objetos e movida para o diretório de quarentena.

Código	Campo	Descrição
FPTH	Caminho do arquivo	O caminho do arquivo da cópia inesperada do objeto.
RSLT	Resultado	Este campo tem o valor 'NENHUM'. RSLT é um campo de mensagem obrigatório, mas não é relevante para esta mensagem. 'NONE' é usado em vez de 'SUCS' para que esta mensagem não seja filtrada.

A mensagem de auditoria SVRU: Object Store Verify Unknown deve ser monitorada de perto. Isso significa que cópias inesperadas de dados de objeto foram detectadas no armazenamento de objetos. Essa situação deve ser investigada imediatamente para determinar como essas cópias foram criadas, pois pode indicar falhas iminentes de hardware.

SYSD: Parada do nó

Quando um serviço é interrompido normalmente, esta mensagem é gerada para indicar que o desligamento foi solicitado. Normalmente, essa mensagem é enviada somente após uma reinicialização subsequente, porque a fila de mensagens de auditoria não é limpa antes do desligamento. Procure a mensagem SYST, enviada no início da sequência de desligamento, se o serviço não tiver sido reiniciado.

Código	Campo	Descrição
RSLT	Desligamento limpo	A natureza do desligamento: SUCS: O sistema foi desligado corretamente.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatórios. O RSLT de um SYSD não pode indicar um desligamento "sujo", porque a mensagem é gerada apenas por desligamentos "limpos".

SYST: Parada do nó

Quando um serviço é interrompido normalmente, esta mensagem é gerada para indicar

que o desligamento foi solicitado e que o serviço iniciou sua sequência de desligamento. SYST pode ser usado para determinar se o desligamento foi solicitado antes do serviço ser reiniciado (ao contrário de SYSD, que normalmente é enviado após a reinicialização do serviço).

Código	Campo	Descrição
RSLT	Desligamento limpo	A natureza do desligamento: SUCS: O sistema foi desligado corretamente.

A mensagem não indica se o servidor host está sendo interrompido, apenas o serviço de relatórios. O código RSLT de uma mensagem SYST não pode indicar um desligamento "sujo", porque a mensagem é gerada apenas por desligamentos "limpos".

SYSU: Início do nó

Quando um serviço é reiniciado, esta mensagem é gerada para indicar se o desligamento anterior foi limpo (comandado) ou desordenado (inesperado).

Código	Campo	Descrição
RSLT	Desligamento limpo	A natureza do desligamento: SUCS: O sistema foi desligado corretamente. DSDN: O sistema não foi desligado corretamente. VRGN: O sistema foi iniciado pela primeira vez após a instalação do servidor (ou reinstalação).

A mensagem não indica se o servidor host foi iniciado, apenas o serviço de relatórios. Esta mensagem pode ser usada para:

- Detecte descontinuidade na trilha de auditoria.
- Determine se um serviço está falhando durante a operação (já que a natureza distribuída do sistema StorageGRID pode mascarar essas falhas). O Gerenciador do Servidor reinicia automaticamente um serviço com falha.

WDEL: Swift EXCLUIR

Quando um cliente Swift emite uma transação DELETE, uma solicitação é feita para remover o objeto ou contêiner especificado. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em contêineres não incluem este campo.

Código	Campo	Descrição
CSIZ	Tamanho do conteúdo	O tamanho do objeto excluído em bytes. Operações em contêineres não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
MTME	Última hora modificada	O registro de data e hora do Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código de resultado	Resultado da transação DELETE. O resultado é sempre: SUCS: Bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
SGRP	Site (Grupo)	Se presente, o objeto foi excluído no site especificado, que não é o site onde o objeto foi ingerido.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
WACC	ID da conta Swift	O ID de conta exclusivo, conforme especificado pelo sistema StorageGRID .
WCON	Contêiner Swift	O nome do contêiner Swift.
WOBJ	Objeto Swift	O identificador de objeto Swift. Operações em contêineres não incluem este campo.

Código	Campo	Descrição
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WGET: GET rápido

Quando um cliente Swift emite uma transação GET, uma solicitação é feita para recuperar um objeto, listar os objetos em um contêiner ou listar os contêineres em uma conta. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em contas e contêineres não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em contas e contêineres não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `` `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). ``
RSLT	Código de resultado	Resultado da transação GET. O resultado é sempre SUCS: bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .

Código	Campo	Descrição
WACC	ID da conta Swift	O ID de conta exclusivo, conforme especificado pelo sistema StorageGRID .
WCON	Contêiner Swift	O nome do contêiner Swift. Operações em contas não incluem este campo.
WOBJ	Objeto Swift	O identificador de objeto Swift. Operações em contas e contêineres não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WHEA: CABEÇA Rápida

Quando um cliente Swift emite uma transação HEAD, uma solicitação é feita para verificar a existência de uma conta, contêiner ou objeto e recuperar quaisquer metadados relevantes. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em contas e contêineres não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em contas e contêineres não incluem este campo.
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `` `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP). ``
RSLT	Código de resultado	Resultado da transação HEAD. O resultado é sempre: SUCS: bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.

Código	Campo	Descrição
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
WACC	ID da conta Swift	O ID de conta exclusivo, conforme especificado pelo sistema StorageGRID .
WCON	Contêiner Swift	O nome do contêiner Swift. Operações em contas não incluem este campo.
WOBJ	Objeto Swift	O identificador de objeto Swift. Operações em contas e contêineres não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

WPUT: PUT rápido

Quando um cliente Swift emite uma transação PUT, uma solicitação é feita para criar um novo objeto ou contêiner. Esta mensagem é emitida pelo servidor se a transação for bem-sucedida.

Código	Campo	Descrição
CBDI	Identificador de bloco de conteúdo	O identificador exclusivo do bloco de conteúdo solicitado. Se o CBID for desconhecido, este campo será definido como 0. Operações em contêineres não incluem este campo.
CSIZ	Tamanho do conteúdo	O tamanho do objeto recuperado em bytes. Operações em contêineres não incluem este campo.

Código	Campo	Descrição
HTRH	Cabeçalho de solicitação HTTP	Lista de nomes e valores de cabeçalhos de solicitações HTTP registrados, conforme selecionados durante a configuração. `X-Forwarded-For`é incluído automaticamente se estiver presente na solicitação e se o `X-Forwarded-For` valor é diferente do endereço IP do remetente da solicitação (campo de auditoria SAIP).
MTME	Última hora modificada	O registro de data e hora do Unix, em microssegundos, indicando quando o objeto foi modificado pela última vez.
RSLT	Código de resultado	Resultado da transação PUT. O resultado é sempre: SUCS: bem-sucedido
SAIP	Endereço IP do cliente solicitante	O endereço IP do aplicativo cliente que fez a solicitação.
TEMPO	Tempo	Tempo total de processamento da solicitação em microssegundos.
TLIP	Endereço IP do balanceador de carga confiável	Se a solicitação foi roteada por um balanceador de carga confiável da Camada 7, o endereço IP do balanceador de carga.
UUID	Identificador Universalmente Único	O identificador do objeto dentro do sistema StorageGRID .
WACC	ID da conta Swift	O ID de conta exclusivo, conforme especificado pelo sistema StorageGRID .
WCON	Contêiner Swift	O nome do contêiner Swift.
WOBJ	Objeto Swift	O identificador de objeto Swift. Operações em contêineres não incluem este campo.
WUSR	Usuário da conta Swift	O nome de usuário da conta Swift que identifica exclusivamente o cliente que realiza a transação.

Informações sobre direitos autorais

Informações sobre marcas comerciais