Revisar los registros de auditoría

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Revisar los registros de auditoría

Mensajes y registros de auditoría

Estas instrucciones contienen información sobre la estructura y el contenido de los mensajes de auditoría y los registros de auditoría de StorageGRID . Puede utilizar esta información para leer y analizar el registro de auditoría de la actividad del sistema.

Estas instrucciones están dirigidas a los administradores responsables de producir informes de actividad y uso del sistema que requieren el análisis de los mensajes de auditoría del sistema StorageGRID .

Para utilizar el archivo de registro de texto, debe tener acceso al recurso compartido de auditoría configurado en el nodo de administración.

Para obtener información sobre cómo configurar los niveles de mensajes de auditoría y utilizar un servidor syslog externo, consulte"Configurar mensajes de auditoría y destinos de registro" .

Auditoría del flujo y retención de mensajes

Todos los servicios de StorageGRID generan mensajes de auditoría durante el funcionamiento normal del sistema. Debe comprender cómo estos mensajes de auditoría se mueven a través del sistema StorageGRID hasta el `audit.log` archivo.

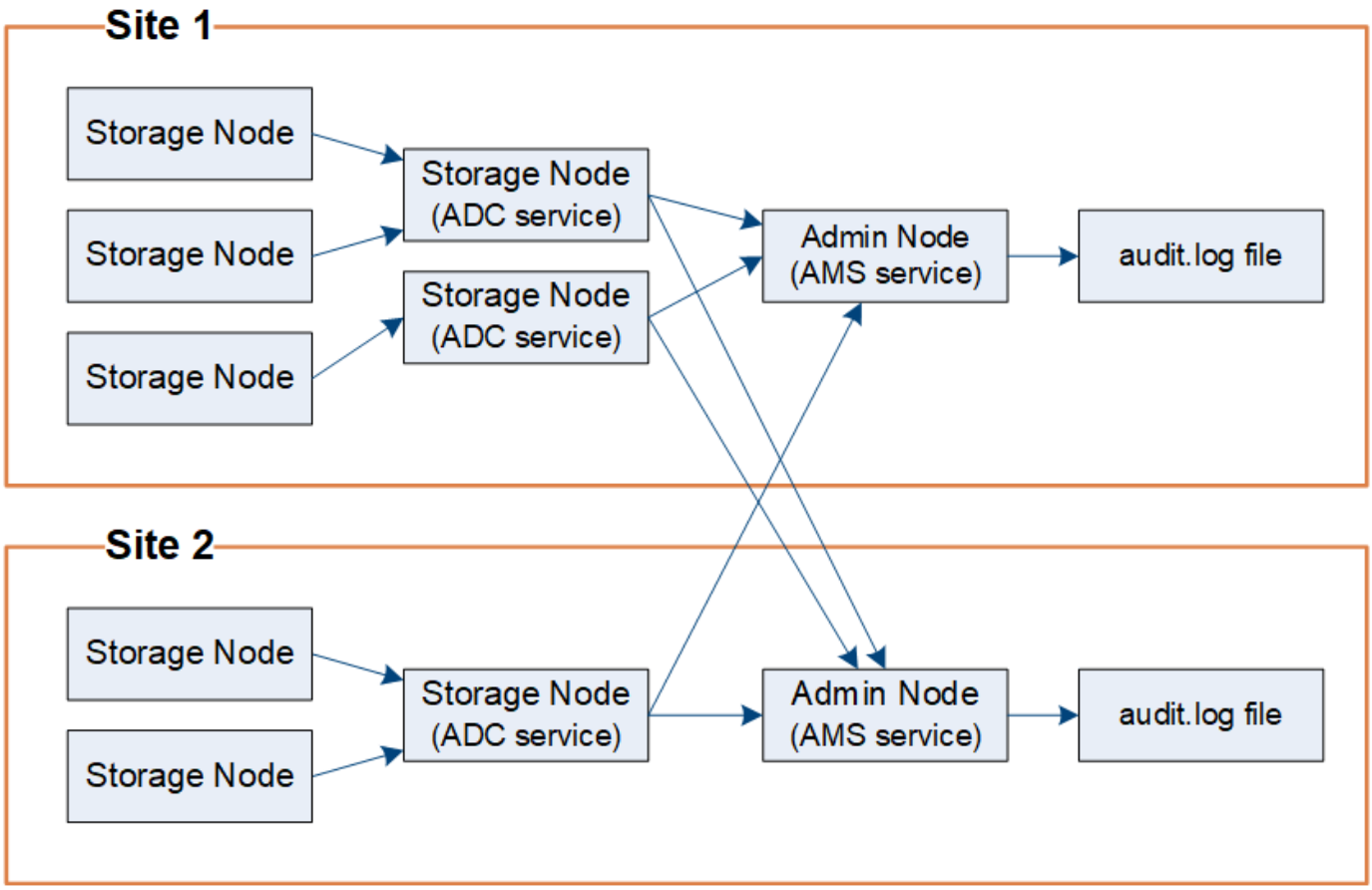
Flujo de mensajes de auditoría

Los mensajes de auditoría son procesados por los nodos de administración y por aquellos nodos de almacenamiento que tienen un servicio de controlador de dominio administrativo (ADC).

Como se muestra en el diagrama de flujo de mensajes de auditoría, cada nodo StorageGRID envía sus mensajes de auditoría a uno de los servicios ADC en el sitio del centro de datos. El servicio ADC se habilita automáticamente para los primeros tres nodos de almacenamiento instalados en cada sitio.

A su vez, cada servicio ADC actúa como un relé y envía su colección de mensajes de auditoría a cada nodo de administración en el sistema StorageGRID , lo que proporciona a cada nodo de administración un registro completo de la actividad del sistema.

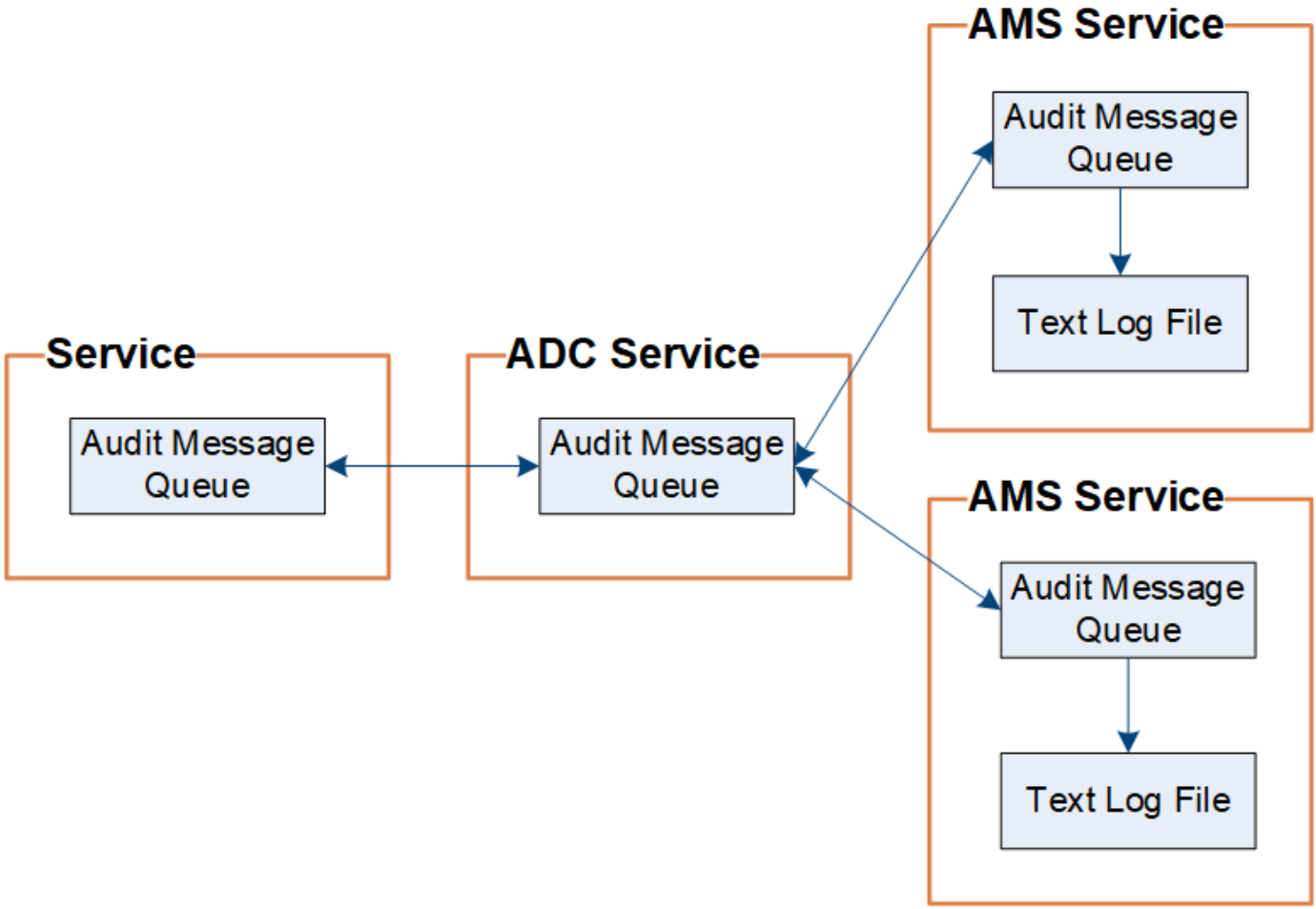
Cada nodo de administración almacena mensajes de auditoría en archivos de registro de texto; el archivo de registro activo se denomina `audit.log` .



Retención de mensajes de auditoría

StorageGRID utiliza un proceso de copia y eliminación para garantizar que no se pierdan mensajes de auditoría antes de que puedan escribirse en el registro de auditoría.

Cuando un nodo genera o retransmite un mensaje de auditoría, el mensaje se almacena en una cola de mensajes de auditoría en el disco del sistema del nodo de la red. Siempre se guarda una copia del mensaje en una cola de mensajes de auditoría hasta que el mensaje se escribe en el archivo de registro de auditoría en el nodo de administración. `/var/local/log` directorio. Esto ayuda a evitar la pérdida de un mensaje de auditoría durante el transporte.



La cola de mensajes de auditoría puede aumentar temporalmente debido a problemas de conectividad de red o capacidad de auditoría insuficiente. A medida que aumentan las colas, consumen más espacio disponible en cada nodo. `/var/local/` directorio. Si el problema persiste y el directorio de mensajes de auditoría de un nodo se llena demasiado, los nodos individuales priorizarán el procesamiento de su trabajo atrasado y quedarán temporalmente no disponibles para nuevos mensajes.

En concreto, es posible que veas los siguientes comportamientos:

- Si el `/var/local/log` Si el directorio utilizado por un nodo de administración se llena, dicho nodo se marcará como no disponible para nuevos mensajes de auditoría hasta que el directorio ya no esté lleno. Las solicitudes de cliente S3 no se ven afectadas. La alarma XAMS (Repositorios de auditoría inaccesibles) se activa cuando un repositorio de auditoría no está disponible.
- Si el `/var/local/` Si el directorio utilizado por un nodo de almacenamiento con el servicio ADC se llena en un 92 %, el nodo se marcará como no disponible para auditar mensajes hasta que el directorio esté lleno solo en un 87 %. Las solicitudes del cliente S3 a otros nodos no se ven afectadas. La alarma NRLY (Relés de auditoría disponibles) se activa cuando los relés de auditoría no están disponibles.

> Si no hay nodos de almacenamiento disponibles con el servicio ADC, los nodos de almacenamiento almacenan los mensajes de auditoría localmente en el `/var/local/log/localaudit.log` archivo.

- Si el `/var/local/` Cuando el directorio utilizado por un nodo de almacenamiento se llena al 85 %, el nodo comenzará a rechazar solicitudes de clientes S3 con `503 Service Unavailable`.

Los siguientes tipos de problemas pueden provocar que las colas de mensajes de auditoría crezcan mucho:

- La interrupción de un nodo de administración o de un nodo de almacenamiento con el servicio ADC. Si uno de los nodos del sistema está inactivo, los nodos restantes pueden quedar atrasados.
- Una tasa de actividad sostenida que excede la capacidad de auditoría del sistema.
- El `/var/local/` El espacio en un nodo de almacenamiento ADC se llena por razones no relacionadas con los mensajes de auditoría. Cuando esto sucede, el nodo deja de aceptar nuevos mensajes de auditoría y prioriza su trabajo pendiente actual, lo que puede provocar retrasos en otros nodos.

Alerta de cola de auditoría grande y alarma de mensajes de auditoría en cola (AMQS)

Para ayudarlo a monitorear el tamaño de las colas de mensajes de auditoría a lo largo del tiempo, la alerta **Cola de auditoría grande** y la alarma AMQS heredada se activan cuando la cantidad de mensajes en una cola de nodo de almacenamiento o en una cola de nodo de administración alcanza ciertos umbrales.

Si se activa la alerta **Cola de auditoría grande** o la alarma AMQS heredada, comience por verificar la carga en el sistema: si hubo una cantidad significativa de transacciones recientes, la alerta y la alarma deberían resolverse con el tiempo y pueden ignorarse.

Si la alerta o alarma persiste y aumenta en gravedad, vea un gráfico del tamaño de la cola. Si el número aumenta de manera constante a lo largo de horas o días, es probable que la carga de auditoría haya excedido la capacidad de auditoría del sistema. Reduzca la tasa de operación del cliente o disminuya la cantidad de mensajes de auditoría registrados cambiando el nivel de auditoría de Escrituras de cliente y Lecturas de cliente a Error o Desactivado. Ver "Configurar mensajes de auditoría y destinos de registro" .

Mensajes duplicados

El sistema StorageGRID adopta un enfoque conservador si ocurre una falla en la red o en un nodo. Por este motivo, podrían existir mensajes duplicados en el registro de auditoría.

Archivo de registro de auditoría de acceso

La parte de auditoría contiene los activos `audit.log` archivo y cualquier archivo de registro de auditoría comprimido. Puede acceder a los archivos de registro de auditoría directamente desde la línea de comando del nodo de administración.

Antes de empezar

- Tienes"permisos de acceso específicos" .
- Debes tener el `Passwords.txt` archivo.
- Debes conocer la dirección IP de un nodo de administración.

Pasos

1. Inicie sesión en un nodo de administración:
   a. Introduzca el siguiente comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a root: `su -`
   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#` .

2. Vaya al directorio que contiene los archivos de registro de auditoría:

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

3. Ver el archivo de registro de auditoría actual o guardado, según sea necesario.

Rotación de archivos de registro de auditoría

Los archivos de registros de auditoría se guardan en un nodo de administración. `/var/local/log` directorio. Los archivos de registro de auditoría activos se denominan `audit.log` .

> Opcionalmente, puede cambiar el destino de los registros de auditoría y enviar información de auditoría a un servidor syslog externo. Los registros locales de registros de auditoría continúan generándose y almacenándose cuando se configura un servidor syslog externo. Ver "Configurar mensajes de auditoría y destinos de registro" .

Una vez al día, el activo `audit.log` El archivo se guarda y se crea uno nuevo. `audit.log` El archivo se inicia. El nombre del archivo guardado indica cuándo se guardó, en el formato *`yyyy-mm-dd.txt`* . Si se crea más de un registro de auditoría en un solo día, los nombres de archivo utilizan la fecha en que se guardó el archivo, más un número, en el formato *`yyyy-mm-dd.txt.n`* . Por ejemplo, `2018-04-15.txt` y `2018-04-15.txt.1` son el primer y segundo archivo de registro creados y guardados el 15 de abril de 2018.

Después de un día, el archivo guardado se comprime y se renombra, en el formato *`yyyy-mm-dd.txt.gz`* , que conserva la fecha original. Con el tiempo, esto genera el consumo del almacenamiento asignado para los registros de auditoría en el nodo de administración. Un script monitorea el consumo de espacio del registro de auditoría y elimina archivos de registro según sea necesario para liberar espacio en el `/var/local/log` directorio. Los registros de auditoría se eliminan según la fecha en que se crearon, siendo los más antiguos los que se eliminan primero. Puedes monitorizar las acciones del script en el siguiente archivo: `/var/local/log/manage-audit.log` .

Este ejemplo muestra el activo `audit.log` archivo, archivo del día anterior(`2018-04-15.txt`), y el archivo comprimido del día anterior(`2018-04-14.txt.gz`).

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

Formato de archivo de registro de auditoría

Formato de archivo de registro de auditoría

Los archivos de registro de auditoría se encuentran en cada nodo de administración y contienen una colección de mensajes de auditoría individuales.

Cada mensaje de auditoría contiene lo siguiente:

- El Tiempo Universal Coordinado (UTC) del evento que activó el mensaje de auditoría (ATIM) en formato ISO 8601, seguido de un espacio:

  YYYY-MM-DDTHH:MM:SS.UUUUUU, dónde *UUUUUU* son microsegundos.

- El mensaje de auditoría en sí, encerrado entre corchetes y comenzando con `AUDT` .

El siguiente ejemplo muestra tres mensajes de auditoría en un archivo de registro de auditoría (se agregan saltos de línea para facilitar la lectura). Estos mensajes se generaron cuando un inquilino creó un depósito S3 y agregó dos objetos a ese depósito.

```
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]]
```

En su formato predeterminado, los mensajes de auditoría en los archivos de registro de auditoría no son fáciles de leer ni interpretar. Puedes utilizar el"herramienta de auditoría y explicación" para obtener resúmenes simplificados de los mensajes de auditoría en el registro de auditoría. Puedes utilizar el"herramienta de suma de auditoría" para resumir cuántas operaciones de escritura, lectura y eliminación se registraron y cuánto tiempo tomaron estas operaciones.

Utilice la herramienta de auditoría y explicación

Puedes utilizar el `audit-explain` herramienta para traducir los mensajes de auditoría

en el registro de auditoría a un formato fácil de leer.

Antes de empezar

- Tienes"permisos de acceso específicos" .
- Debes tener el `Passwords.txt` archivo.
- Debe conocer la dirección IP del nodo de administración principal.

Acerca de esta tarea

El `audit-explain` La herramienta, disponible en el nodo de administración principal, proporciona resúmenes simplificados de los mensajes de auditoría en un registro de auditoría.

> ⓘ El `audit-explain` La herramienta está destinada principalmente a ser utilizada por el soporte técnico durante operaciones de resolución de problemas. Tratamiento `audit-explain` Las consultas pueden consumir una gran cantidad de energía de la CPU, lo que podría afectar las operaciones de StorageGRID .

Este ejemplo muestra una salida típica del `audit-explain` herramienta. Estos cuatro"ESPOLVO" Se generaron mensajes de auditoría cuando el inquilino S3 con ID de cuenta 92484777680322627870 utilizó solicitudes S3 PUT para crear un depósito llamado "bucket1" y agregar tres objetos a ese depósito.

```
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
```

El `audit-explain` La herramienta puede hacer lo siguiente:

- Procesar registros de auditoría simples o comprimidos. Por ejemplo:

  ```
  audit-explain audit.log

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

- Procesar múltiples archivos simultáneamente. Por ejemplo:

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

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

- Acepte la entrada de una tubería, lo que le permite filtrar y preprocesar la entrada utilizando el `grep` comando u otros medios. Por ejemplo:

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

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

Debido a que los registros de auditoría pueden ser muy grandes y lentos de analizar, puede ahorrar tiempo filtrando las partes que desea ver y ejecutando `audit-explain` en las partes, en lugar de en todo el archivo.

> El `audit-explain` La herramienta no acepta archivos comprimidos como entrada canalizada. Para procesar archivos comprimidos, proporcione sus nombres de archivo como argumentos de línea de comando o utilice el `zcat` herramienta para descomprimir los archivos primero. Por ejemplo:
>
> ```
> zcat audit.log.gz | audit-explain
> ```

Utilice el `help (-h)` Opción para ver las opciones disponibles. Por ejemplo:

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

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a root: `su -`
   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

   Cuando inicia sesión como root, el mensaje cambia de `$` a `#` .
2. Introduzca el siguiente comando, donde `/var/local/log/audit.log` representa el nombre y la ubicación del archivo o archivos que desea analizar:

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

   El `audit-explain` La herramienta imprime interpretaciones legibles por humanos de todos los mensajes en el archivo o archivos especificados.

   > Para reducir la longitud de las líneas y facilitar la legibilidad, las marcas de tiempo no se muestran de forma predeterminada. Si desea ver las marcas de tiempo, utilice la marca de tiempo(`-t`) opción.

Utilice la herramienta de suma de auditoría

Puedes utilizar el `audit-sum` herramienta para contar los mensajes de auditoría de escritura, lectura, encabezado y eliminación y para ver el tiempo mínimo, máximo y promedio (o tamaño) para cada tipo de operación.

Antes de empezar

- Tienes"permisos de acceso específicos" .
- Debes tener el `Passwords.txt` archivo.
- Debe conocer la dirección IP del nodo de administración principal.

Acerca de esta tarea

El `audit-sum` La herramienta, disponible en el nodo de administración principal, resume cuántas operaciones de escritura, lectura y eliminación se registraron y cuánto tiempo tomaron estas operaciones.

> El `audit-sum` La herramienta está destinada principalmente a ser utilizada por el soporte técnico durante operaciones de resolución de problemas. Tratamiento `audit-sum` Las consultas pueden consumir una gran cantidad de energía de la CPU, lo que podría afectar las operaciones de StorageGRID .

Este ejemplo muestra una salida típica del `audit-sum` herramienta. Este ejemplo muestra cuánto tiempo tomaron las operaciones del 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
```

El `audit-sum` La herramienta proporciona recuentos y tiempos para los siguientes mensajes de auditoría de S3, Swift e ILM en un registro de auditoría.

> Los códigos de auditoría se eliminan del producto y de la documentación a medida que las funciones quedan obsoletas. Si encuentra un código de auditoría que no aparece aquí, consulte las versiones anteriores de este tema para ver versiones anteriores de SG. Por ejemplo, "Documentación sobre el uso de la herramienta de suma de auditoría de StorageGRID 11.8" .

Código	Descripción	Referirse a
IDEL	Eliminación iniciada por ILM: registra cuándo ILM inicia el proceso de eliminación de un objeto.	"IDEL: Eliminación iniciada por ILM"
SDEL	S3 ELIMINAR: registra una transacción exitosa para eliminar un objeto o depósito.	"SDEL: S3 ELIMINAR"
SGET	S3 GET: registra una transacción exitosa para recuperar un objeto o enumerar los objetos en un depósito.	"SGET: S3 OBTENER"
KARITÉ	S3 HEAD: Registra una transacción exitosa para verificar la existencia de un objeto o depósito.	"SHEA: CABEZA T3"

Código	Descripción	Referirse a
ESPOLVO	S3 PUT: Registra una transacción exitosa para crear un nuevo objeto o depósito.	"SPUT: S3 PONER"
WDEL	Swift DELETE: registra una transacción exitosa para eliminar un objeto o contenedor.	"WDEL: Eliminación rápida"
WGET	Swift GET: registra una transacción exitosa para recuperar un objeto o enumerar los objetos en un contenedor.	"WGET: Obtención rápida"
TRIGO	Swift HEAD: registra una transacción exitosa para verificar la existencia de un objeto o contenedor.	"WHEA: CABEZA Veloz"
WPUT	Swift PUT: registra una transacción exitosa para crear un nuevo objeto o contenedor.	"WPUT: PUT rápido"

El `audit-sum` La herramienta puede hacer lo siguiente:

- Procesar registros de auditoría simples o comprimidos. Por ejemplo:

```
audit-sum audit.log

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

- Procesar múltiples archivos simultáneamente. Por ejemplo:

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

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

- Acepte la entrada de una tubería, lo que le permite filtrar y preprocesar la entrada utilizando el `grep` comando u otros medios. Por ejemplo:

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

grep bucket1 audit.log | audit-sum

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

> Esta herramienta no acepta archivos comprimidos como entrada canalizada. Para procesar archivos comprimidos, proporcione sus nombres de archivo como argumentos de línea de comando o utilice el `zcat` herramienta para descomprimir los archivos primero. Por ejemplo:
>
> ```
> audit-sum audit.log.gz
>
> zcat audit.log.gz | audit-sum
> ```

Puede utilizar las opciones de la línea de comandos para resumir las operaciones en los depósitos por separado de las operaciones en los objetos o para agrupar resúmenes de mensajes por nombre de depósito, por período de tiempo o por tipo de destino. De forma predeterminada, los resúmenes muestran el tiempo de operación mínimo, máximo y promedio, pero puede utilizar el `size (-s)` Opción para mirar el tamaño del

objeto en su lugar.

Utilice el `help (-h)` Opción para ver las opciones disponibles. Por ejemplo:

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

Pasos

1. Inicie sesión en el nodo de administración principal:
   a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
   b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a root: `su -`
   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

      Cuando inicia sesión como root, el mensaje cambia de `$` a `#` .

2. Si desea analizar todos los mensajes relacionados con las operaciones de escritura, lectura, encabezado y eliminación, siga estos pasos:
   a. Introduzca el siguiente comando, donde `/var/local/log/audit.log` representa el nombre y la ubicación del archivo o archivos que desea analizar:

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

      Este ejemplo muestra una salida típica del `audit-sum` herramienta. Este ejemplo muestra cuánto tiempo tomaron las operaciones del 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
      ```

      En este ejemplo, las operaciones SGET (S3 GET) son las más lentas en promedio, con 1,13 segundos, pero las operaciones SGET y SPUT (S3 PUT) muestran tiempos de peor caso prolongados de aproximadamente 1770 segundos.

   b. Para mostrar las 10 operaciones de recuperación más lentas, utilice el comando grep para seleccionar solo mensajes SGET y agregar la opción de salida larga(`-l`) para incluir rutas de objetos:

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

Los resultados incluyen el tipo (objeto o depósito) y la ruta, lo que le permite buscar en el registro de auditoría otros mensajes relacionados con estos objetos particulares.

```
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
```

+ En este ejemplo de salida, puede ver que las tres solicitudes GET de S3 más lentas fueron para objetos de aproximadamente 5 GB de tamaño, lo cual es mucho más grande que los otros objetos. El gran tamaño explica los tiempos de recuperación lentos en el peor de los casos.

3. Si desea determinar qué tamaños de objetos se están ingiriendo y recuperando de su cuadrícula, utilice la opción de tamaño(`-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
```

En este ejemplo, el tamaño de objeto promedio para SPUT es inferior a 2,5 MB, pero el tamaño promedio para SGET es mucho mayor. La cantidad de mensajes SPUT es mucho mayor que la cantidad de mensajes SGET, lo que indica que la mayoría de los objetos nunca se recuperan.

4. Si desea determinar si las recuperaciones fueron lentas ayer:

   a. Emita el comando en el registro de auditoría apropiado y utilice la opción agrupar por tiempo(`-gt`), seguido del período de tiempo (por ejemplo, 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
```

Estos resultados muestran que el tráfico GET de S3 aumentó entre las 06:00 y las 07:00. Los tiempos máximos y promedio también son considerablemente más altos en estos momentos y no aumentan gradualmente a medida que aumenta el recuento. Esto sugiere que se excedió la capacidad en algún lugar, quizás en la red o en la capacidad de la red para procesar solicitudes.

b. Para determinar qué tamaño de objetos se recuperaron cada hora ayer, agregue la opción de tamaño(`-s`) al 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
```

Estos resultados indican que algunas recuperaciones muy grandes ocurrieron cuando el tráfico de recuperación general estaba en su máximo.

c. Para ver más detalles, utilice el"herramienta de auditoría y explicación" para revisar todas las operaciones de SGET durante esa hora:

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

Si se espera que la salida del comando grep tenga muchas líneas, agregue el `less` comando para mostrar el contenido del archivo de registro de auditoría una página (una pantalla) a la vez.

5. Si desea determinar si las operaciones SPUT en depósitos son más lentas que las operaciones SPUT en objetos:

a. Comience usando el `-go` opción, que agrupa los mensajes para operaciones de objetos y depósitos por separado:

```
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
```

Los resultados muestran que las operaciones SPUT para contenedores tienen características de rendimiento diferentes a las de las operaciones SPUT para objetos.

b. Para determinar qué buckets tienen las operaciones SPUT más lentas, utilice el `-gb` opción, que agrupa los mensajes por contenedor:

```
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 qué depósitos tienen el tamaño de objeto SPUT más grande, utilice ambos `-gb` y el `-s` opciones:

```
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 del mensaje de auditoría

Formato del mensaje de auditoría

Los mensajes de auditoría intercambiados dentro del sistema StorageGRID incluyen información estándar común a todos los mensajes y contenido específico que describe el evento o la actividad que se informa.

Si la información resumida proporcionada por el"auditoría-explicación" y"suma de auditoría" Si las herramientas son insuficientes, consulte esta sección para comprender el formato general de todos los mensajes de auditoría.

El siguiente es un ejemplo de mensaje de auditoría tal como podría aparecer en el archivo de registro de auditoría:

```
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 mensaje de auditoría contiene una cadena de elementos de atributos. La cadena completa está entre corchetes.(`[ ]`), y cada elemento de atributo en la cadena tiene las siguientes características:

- Entre paréntesis `[ ]`
- Introducido por la cadena `AUDT` , lo que indica un mensaje de auditoría
- Sin delimitadores (sin comas ni espacios) antes ni después
- Terminado por un carácter de avance de línea `\n`

Cada elemento incluye un código de atributo, un tipo de dato y un valor que se informan en este formato:

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

La cantidad de elementos de atributo en el mensaje depende del tipo de evento del mensaje. Los elementos de atributo no se enumeran en ningún orden particular.

La siguiente lista describe los elementos de atributo:

- `ATTR`es un código de cuatro caracteres para el atributo que se informa. Hay algunos atributos que son comunes a todos los mensajes de auditoría y otros que son específicos del evento.
- `type`es un identificador de cuatro caracteres del tipo de datos de programación del valor, como UI64, FC32, etc. El tipo está entre paréntesis. `( ).
- `value`es el contenido del atributo, normalmente un valor numérico o de texto. Los valores siempre siguen a dos puntos(:`). Los valores del tipo de datos CSTR están rodeados por comillas dobles " ".

Tipos de datos

Se utilizan diferentes tipos de datos para almacenar información en los mensajes de auditoría.

Tipo	Descripción
UI32	Entero largo sin signo (32 bits); puede almacenar los números del 0 al 4.294.967.295.
UI64	Entero doble largo sin signo (64 bits); puede almacenar los números del 0 al 18.446.744.073.709.551.615.
FC32	Constante de cuatro caracteres; un valor entero sin signo de 32 bits representado como cuatro caracteres ASCII como "ABCD".
iPad	Se utiliza para direcciones IP.
CSTR	Una matriz de longitud variable de caracteres UTF-8. Los caracteres se pueden escapar con las siguientes convenciones: • La barra invertida es \\. • El retorno de carro es \r. • Las comillas dobles son \". • El salto de línea (nueva línea) es \n. • Los caracteres se pueden reemplazar por sus equivalentes hexadecimales (en el formato \xHH, donde HH es el valor hexadecimal que representa el carácter).

Datos específicos del evento

Cada mensaje de auditoría en el registro de auditoría registra datos específicos de un evento del sistema.

Tras la inauguración `[AUDT:` contenedor que identifica el mensaje en sí, el siguiente conjunto de atributos proporciona información sobre el evento o la acción descrita por el mensaje de auditoría. Estos atributos se resaltan en el siguiente ejemplo:

```
2018-12-05T08:24:45.921845 [AUDT:*\[RSLT\(FC32\):SUCS\]*
\[TIEMPO\(UI64\):11454\]\[SAIP\(IPAD\):"10.224.0.100"\]\[S3AI\(CSTR\):"60025621595611246499"\]
\[SACC\(CSTR\):"cuenta"\]\[S3AK\(CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsK
JA=="\] \[SUSR\(CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\(CSTR\):"60025621595611246499"\]\[SBAC\(CSTR\):"cuenta"\]\[S3BK\(CSTR\):"depósito"\]
\[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]]
```

El `ATYP` El elemento (subrayado en el ejemplo) identifica qué evento generó el mensaje. Este mensaje de ejemplo incluye el"KARITÉ" código de mensaje ([ATYP(FC32):SHEA]), que indica que fue generado por una solicitud S3 HEAD exitosa.

Elementos comunes en los mensajes de auditoría

Todos los mensajes de auditoría contienen los elementos comunes.

Código	Tipo	Descripción
EN MEDIO DE	FC32	ID del módulo: un identificador de cuatro caracteres del ID del módulo que generó el mensaje. Esto indica el segmento de código dentro del cual se generó el mensaje de auditoría.
ANID	UI32	ID de nodo: el ID del nodo de la red asignado al servicio que generó el mensaje. A cada servicio se le asigna un identificador único en el momento en que se configura e instala el sistema StorageGRID . Esta identificación no se puede cambiar.
ASES	UI64	Identificador de sesión de auditoría: en versiones anteriores, este elemento indicaba el momento en el que se inicializaba el sistema de auditoría después de iniciarse el servicio. Este valor de tiempo se midió en microsegundos desde la época del sistema operativo (00:00:00 UTC del 1 de enero de 1970). **Nota:** Este elemento está obsoleto y ya no aparece en los mensajes de auditoría.

Código	Tipo	Descripción
ASQN	UI64	Recuento de secuencia: en versiones anteriores, este contador se incrementaba para cada mensaje de auditoría generado en el nodo de la red (ANID) y se restablecía a cero al reiniciar el servicio. **Nota:** Este elemento está obsoleto y ya no aparece en los mensajes de auditoría.
ATID	UI64	ID de seguimiento: un identificador que comparte el conjunto de mensajes que se activaron mediante un solo evento.
ATIM	UI64	Marca de tiempo: la hora en que se generó el evento que activó el mensaje de auditoría, medido en microsegundos desde la época del sistema operativo (00:00:00 UTC del 1 de enero de 1970). Tenga en cuenta que la mayoría de las herramientas disponibles para convertir la marca de tiempo a fecha y hora locales se basan en milisegundos. Podría ser necesario redondear o truncar la marca de tiempo registrada. La hora legible por humanos que aparece al comienzo del mensaje de auditoría en el `audit.log` El archivo es el atributo ATIM en formato ISO 8601. La fecha y la hora se representan como *`YYYY-MMDDTHH:MM:SS.UUUUUU`* , donde el `T` es un carácter de cadena literal que indica el comienzo del segmento de tiempo de la fecha. *`UUUUUU`* son microsegundos.
ATYP	FC32	Tipo de evento: un identificador de cuatro caracteres del evento que se está registrando. Esto regula el contenido de "carga útil" del mensaje: los atributos que se incluyen.
AFIRMAR	UI32	Versión: La versión del mensaje de auditoría. A medida que el software StorageGRID evoluciona, las nuevas versiones de los servicios podrían incorporar nuevas funciones en los informes de auditoría. Este campo permite la compatibilidad con versiones anteriores del servicio AMS para procesar mensajes de versiones anteriores de los servicios.
RSLT	FC32	Resultado: El resultado de un evento, proceso o transacción. Si no es relevante para un mensaje, se utiliza NONE en lugar de SUCS para que el mensaje no se filtre accidentalmente.

Ejemplos de mensajes de auditoría

Puede encontrar información detallada en cada mensaje de auditoría. Todos los mensajes de auditoría utilizan el mismo formato.

El siguiente es un ejemplo de mensaje de auditoría tal como podría aparecer en el `audit.log` archivo:

```
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]]
```

El mensaje de auditoría contiene información sobre el evento que se está registrando, así como información sobre el mensaje de auditoría en sí.

Para identificar qué evento registra el mensaje de auditoría, busque el atributo ATYP (resaltado a continuación):

```
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]]
```

El valor del atributo ATYP es SPUT. "ESPOLVO" representa una transacción S3 PUT, que registra la ingesta de un objeto en un depósito.

El siguiente mensaje de auditoría también muestra el depósito al que está asociado el objeto:

```
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 descubrir cuándo ocurrió el evento PUT, observe la marca de tiempo del Tiempo Universal Coordinado (UTC) al comienzo del mensaje de auditoría. Este valor es una versión legible para humanos del atributo ATIM del mensaje de auditoría en sí:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM registra el tiempo, en microsegundos, desde el comienzo de la época UNIX. En el ejemplo, el valor `1405631878959669` se traduce al jueves, 17 de julio de 2014 21:17:59 UTC.

Mensajes de auditoría y el ciclo de vida de los objetos

¿Cuándo se generan los mensajes de auditoría?

Los mensajes de auditoría se generan cada vez que se ingiere, recupera o elimina un objeto. Puede identificar estas transacciones en el registro de auditoría ubicando los mensajes de auditoría específicos de la API de S3.

Los mensajes de auditoría están vinculados a través de identificadores específicos de cada protocolo.

Protocolo	Código
Vinculación de operaciones S3	S3BK (cubo), S3KY (llave) o ambos
Vinculación de operaciones Swift	WCON (contenedor), WOBJ (objeto) o ambos
Vinculación de operaciones internas	CBID (identificador interno del objeto)

Momento de los mensajes de auditoría

Debido a factores como las diferencias de tiempo entre los nodos de la red, el tamaño de los objetos y los retrasos de la red, el orden de los mensajes de auditoría generados por los diferentes servicios puede variar del que se muestra en los ejemplos de esta sección.

Transacciones de ingesta de objetos

Puede identificar las transacciones de ingesta del cliente en el registro de auditoría ubicando los mensajes de auditoría específicos de la API de S3.

No todos los mensajes de auditoría generados durante una transacción de ingesta se enumeran en las siguientes tablas. Solo se incluyen los mensajes necesarios para rastrear la transacción de ingesta.

Mensajes de auditoría de ingesta de S3

Código	Nombre	Descripción	Rastro	Ver
ESPOLVO	Transacción PUT S3	Se ha completado exitosamente una transacción de ingesta S3 PUT.	CBID, S3BK, S3KY	"SPUT: S3 PONER"
ORLM	Reglas de objeto cumplidas	La política de ILM se ha cumplido para este objeto.	CBD	"ORLM: Se cumplen las reglas de objeto"

Mensajes de auditoría de ingesta de Swift

Código	Nombre	Descripción	Rastro	Ver
WPUT	Transacción PUT rápida	Se ha completado exitosamente una transacción de ingesta Swift PUT.	CBID, WCON, WOBJ	"WPUT: PUT rápido"
ORLM	Reglas de objeto cumplidas	La política de ILM se ha cumplido para este objeto.	CBD	"ORLM: Se cumplen las reglas de objeto"

Ejemplo: ingesta de objetos S3

La serie de mensajes de auditoría a continuación es un ejemplo de los mensajes de auditoría generados y guardados en el registro de auditoría cuando un cliente S3 ingiere un objeto en un nodo de almacenamiento (servicio LDR).

En este ejemplo, la política ILM activa incluye la regla ILM Hacer 2 copias.

> No todos los mensajes de auditoría generados durante una transacción se enumeran en el siguiente ejemplo. Solo se enumeran aquellos relacionados con la transacción de ingesta S3 (SPUT).

Este ejemplo supone que previamente se ha creado un bucket S3.

SPUT: S3 PONER

El mensaje SPUT se genera para indicar que se ha emitido una transacción S3 PUT para crear un objeto en un depósito 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: Se cumplen las reglas de objeto

El mensaje ORLM indica que se ha cumplido la política ILM para este objeto. El mensaje incluye el CBID del objeto y el nombre de la regla ILM que se aplicó.

Para los objetos replicados, el campo LOCS incluye el ID del nodo LDR y el ID del volumen de las ubicaciones de los objetos.

```
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 los objetos con codificación de borrado, el campo LOCS incluye el ID del perfil de codificación de borrado y el ID del grupo de codificación de borrado.

```
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]]
```

El campo PATH incluye información de clave y depósito S3 o información de objeto y contenedor Swift, según qué API se utilizó.

```
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]]
```

Transacciones de eliminación de objetos

Puede identificar transacciones de eliminación de objetos en el registro de auditoría ubicando los mensajes de auditoría específicos de la API de S3.

No todos los mensajes de auditoría generados durante una transacción de eliminación aparecen en las siguientes tablas. Sólo se incluyen los mensajes necesarios para rastrear la transacción de eliminación.

Mensajes de auditoría de eliminación de S3

Código	Nombre	Descripción	Rastro	Ver
SDEL	S3 Eliminar	Solicitud realizada para eliminar el objeto de un depósito.	CBD, S3KY	"SDEL: S3 ELIMINAR"

Eliminar mensajes de auditoría de Swift

Código	Nombre	Descripción	Rastro	Ver
WDEL	Eliminación rápida	Solicitud realizada para eliminar el objeto de un contenedor, o el contenedor.	CBDI, WOBJ	"WDEL: Eliminación rápida"

Ejemplo: eliminación de objetos S3

Cuando un cliente S3 elimina un objeto de un nodo de almacenamiento (servicio LDR), se genera un mensaje de auditoría y se guarda en el registro de auditoría.

> No todos los mensajes de auditoría generados durante una transacción de eliminación se enumeran en el siguiente ejemplo. Solo se enumeran aquellos relacionados con la transacción de eliminación S3 (SDEL).

SDEL: S3 Eliminar

La eliminación de objetos comienza cuando el cliente envía una solicitud DeleteObject a un servicio LDR. El mensaje contiene el depósito desde el cual eliminar el objeto y la clave S3 del objeto, que se utiliza para identificarlo.

```
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]]
```

Transacciones de recuperación de objetos

Puede identificar transacciones de recuperación de objetos en el registro de auditoría ubicando mensajes de auditoría específicos de la API de S3.

No todos los mensajes de auditoría generados durante una transacción de recuperación se enumeran en las siguientes tablas. Sólo se incluyen los mensajes necesarios para rastrear la transacción recuperada.

Mensajes de auditoría de recuperación de S3

Código	Nombre	Descripción	Rastro	Ver
SGET	S3 GET	Solicitud realizada para recuperar un objeto de un depósito.	CBID, S3BK, S3KY	"SGET: S3 OBTENER"

Mensajes de auditoría de recuperación rápida

Código	Nombre	Descripción	Rastro	Ver
WGET	Obtener rápidamente	Solicitud realizada para recuperar un objeto de un contenedor.	CBID, WCON, WOBJ	"WGET: Obtención rápida"

Ejemplo: recuperación de objetos S3

Cuando un cliente S3 recupera un objeto de un nodo de almacenamiento (servicio LDR), se genera un mensaje de auditoría y se guarda en el registro de auditoría.

Tenga en cuenta que no todos los mensajes de auditoría generados durante una transacción aparecen en el siguiente ejemplo. Sólo se enumeran aquellos relacionados con la transacción de recuperación S3 (SGET).

SGET: S3 OBTENER

La recuperación de objetos comienza cuando el cliente envía una solicitud GetObject a un servicio LDR. El mensaje contiene el depósito desde el cual recuperar el objeto y la clave S3 del objeto, que se utiliza para identificarlo.

```
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]
]
```

Si la política del depósito lo permite, un cliente puede recuperar objetos de forma anónima o puede recuperar objetos de un depósito que sea propiedad de una cuenta de inquilino diferente. El mensaje de auditoría contiene información sobre la cuenta de inquilino del propietario del depósito para que pueda realizar un seguimiento de estas solicitudes anónimas y entre cuentas.

En el siguiente mensaje de ejemplo, el cliente envía una solicitud GetObject para un objeto almacenado en un depósito que no es de su propiedad. Los valores para SBAI y SBAC registran el ID y el nombre de la cuenta de inquilino del propietario del depósito, que difieren del ID y el nombre de la cuenta de inquilino del cliente registrados en S3AI y 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]]
```

Ejemplo: S3 Seleccionar un objeto

Cuando un cliente S3 emite una consulta S3 Select sobre un objeto, se generan mensajes de auditoría y se guardan en el registro de auditoría.

Tenga en cuenta que no todos los mensajes de auditoría generados durante una transacción aparecen en el siguiente ejemplo. Solo se enumeran aquellos relacionados con la transacción S3 Select (SelectObjectContent).

Cada consulta genera dos mensajes de auditoría: uno que realiza la autorización de la solicitud S3 Select (el campo S3SR está configurado como "select") y una operación GET estándar posterior que recupera los datos del almacenamiento durante el procesamiento.

```
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):1363009709396895985]]
```

```
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]]
```

Mensajes de actualización de metadatos

Los mensajes de auditoría se generan cuando un cliente S3 actualiza los metadatos de un objeto.

Mensajes de auditoría de actualización de metadatos de S3

Código	Nombre	Descripción	Rastro	Ver
SUPD	Metadatos S3 actualizados	Se genera cuando un cliente S3 actualiza los metadatos de un objeto ingerido.	CBID, S3KY, HTRH	"SUPD: Metadatos S3 actualizados"

Ejemplo: actualización de metadatos de S3

El ejemplo muestra una transacción exitosa para actualizar los metadatos de un objeto S3 existente.

SUPD: Actualización de metadatos S3

El cliente S3 realiza una solicitud (SUPD) para actualizar los metadatos especificados(`x-amz-meta-\*`) para el objeto S3 (S3KY). En este ejemplo, los encabezados de solicitud se incluyen en el campo HTRH porque se ha configurado como un encabezado de protocolo de auditoría (**CONFIGURACIÓN** > **Monitoreo** > **Servidor de auditoría y syslog**). Ver "Configurar mensajes de auditoría y destinos de registro" .

```
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]]
```

Mensajes de auditoría

Descripciones de los mensajes de auditoría

En las siguientes secciones se enumeran descripciones detalladas de los mensajes de auditoría devueltos por el sistema. Cada mensaje de auditoría aparece primero en una tabla que agrupa los mensajes relacionados según la clase de actividad que representa el mensaje. Estas agrupaciones son útiles tanto para comprender los tipos de actividades que se auditan como para seleccionar el tipo de filtrado de mensajes de auditoría deseado.

Los mensajes de auditoría también se enumeran en orden alfabético por sus códigos de cuatro caracteres. Esta lista alfabética le permite encontrar información sobre mensajes específicos.

Los códigos de cuatro caracteres utilizados en este capítulo son los valores ATYP que se encuentran en los mensajes de auditoría, como se muestra en el siguiente mensaje de ejemplo:

```
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 obtener información sobre cómo configurar los niveles de mensajes de auditoría, cambiar los destinos de los registros y usar un servidor syslog externo para su información de auditoría, consulte"Configurar mensajes de auditoría y destinos de registro"

Categorías de mensajes de auditoría

Mensajes de auditoría del sistema

Los mensajes de auditoría que pertenecen a la categoría de auditoría del sistema se utilizan para eventos relacionados con el sistema de auditoría en sí, estados de los nodos de la red, actividad de tareas de todo el sistema (tareas de la red) y operaciones de respaldo de servicio.

Código	Título y descripción del mensaje	Ver
ECMC	Fragmento de datos codificado por borrado faltante: indica que se ha detectado un fragmento de datos codificado por borrado faltante.	"ECMC: Fragmento de datos con código de borrado faltante"
ECOC	Fragmento de datos codificado por borrado corrupto: indica que se ha detectado un fragmento de datos codificado por borrado corrupto.	"ECOC: Fragmento de datos corruptos codificados por borrado"
ETAF	Error de autenticación de seguridad: falló un intento de conexión mediante Seguridad de la capa de transporte (TLS).	"ETAF: Falló la autenticación de seguridad"
GNRG	Registro GNDS: Un servicio actualiza o registra información sobre sí mismo en el sistema StorageGRID .	"GNRG: Registro GNDS"
GNUR	Anulación del registro de GNDS: un servicio se ha anulado su registro en el sistema StorageGRID .	"GNUR: Anulación del registro de GNDS"
GTED	Tarea de cuadrícula finalizada: el servicio CMN terminó de procesar la tarea de cuadrícula.	"GTED: Tarea de cuadrícula finalizada"
GTST	Tarea de cuadrícula iniciada: el servicio CMN comenzó a procesar la tarea de cuadrícula.	"GTST: Tarea de cuadrícula iniciada"
GTSU	Tarea de cuadrícula enviada: se envió una tarea de cuadrícula al servicio CMN.	"GTSU: Tarea de cuadrícula enviada"

Código	Título y descripción del mensaje	Ver
LLST	Ubicación perdida: este mensaje de auditoría se genera cuando se pierde una ubicación.	"LLST: Ubicación perdida"
OLST	Objeto perdido: un objeto solicitado no se puede ubicar dentro del sistema StorageGRID .	"OLST: El sistema detectó un objeto perdido"
Tristeza	Deshabilitar auditoría de seguridad: se desactivó el registro de mensajes de auditoría.	"SADD: Desactivación de auditoría de seguridad"
SADE	Habilitar auditoría de seguridad: se ha restaurado el registro de mensajes de auditoría.	"SADE: Habilitación de auditoría de seguridad"
SVRF	Error de verificación del almacén de objetos: un bloque de contenido no pasó las verificaciones de verificación.	"SVRF: Error en la verificación del almacén de objetos"
Unidad de Registro de Víctimas de Violencia Doméstica	Verificación de almacén de objetos desconocido: se detectaron datos de objetos inesperados en el almacén de objetos.	"SVRU: Verificación de almacén de objetos desconocida"
Distrito Escolar Unificado de Syracuse	Parada de nodo: se solicitó un apagado.	"SYSD: Parada de nodo"
SISTEMA	Detención de nodo: un servicio inició una detención elegante.	"SYST: Nodo deteniéndose"
SYSU	Inicio de nodo: se inició un servicio; la naturaleza del apagado anterior se indica en el mensaje.	"SYSU: Inicio del nodo"

Mensajes de auditoría de almacenamiento de objetos

Los mensajes de auditoría que pertenecen a la categoría de auditoría de almacenamiento de objetos se utilizan para eventos relacionados con el almacenamiento y la administración de objetos dentro del sistema StorageGRID . Estos incluyen almacenamiento y recuperación de objetos, transferencias de nodo de red a nodo de red y verificaciones.

Los códigos de auditoría se eliminan del producto y de la documentación a medida que las funciones quedan obsoletas. Si encuentra un código de auditoría que no aparece aquí, consulte las versiones anteriores de este tema para ver versiones anteriores de SG. Por ejemplo, "Mensajes de auditoría de almacenamiento de objetos de StorageGRID 11.8" .

Código	Descripción	Ver
HERMANO	Solicitud de solo lectura de depósito: un depósito ingresó o salió del modo de solo lectura.	"BROR: Solicitud de solo lectura de depósito"

Código	Descripción	Ver
CBSE	Fin de envío de objeto: la entidad de origen completó una operación de transferencia de datos de un nodo de la red a otro nodo de la red.	"CBSE: Fin de envío de objetos"
CBRE	Fin de recepción del objeto: la entidad de destino completó una operación de transferencia de datos de un nodo de la red a otro nodo de la red.	"CBRE: Extremo de recepción de objetos"
CGRR	Solicitud de replicación entre redes: StorageGRID intentó una operación de replicación entre redes para replicar objetos entre depósitos en una conexión de federación de redes.	"CGRR: Solicitud de replicación entre redes"
EBDL	Eliminar depósito vacío: el escáner ILM eliminó un objeto en un depósito que está eliminando todos los objetos (realizando una operación de depósito vacío).	"EBDL: Eliminar depósito vacío"
EBKR	Solicitud de depósito vacío: un usuario envió una solicitud para activar o desactivar el depósito vacío (es decir, para eliminar objetos del depósito o para dejar de eliminar objetos).	"EBKR: Solicitud de cubo vacío"
SCMT	Confirmación de almacén de objetos: se almacenó y verificó completamente un bloque de contenido y ahora se puede solicitar.	"SCMT: Solicitud de confirmación del almacén de objetos"
SREM	Eliminar almacén de objetos: se eliminó un bloque de contenido de un nodo de la cuadrícula y ya no se puede solicitar directamente.	"SREM: Eliminar almacén de objetos"

El cliente lee mensajes de auditoría

Los mensajes de auditoría de lectura del cliente se registran cuando una aplicación cliente S3 realiza una solicitud para recuperar un objeto.

Código	Descripción	Utilizado por	Ver
S3SL	Solicitud de selección S3: registra una finalización después de que se haya devuelto una solicitud de selección S3 al cliente. El mensaje S3SL puede incluir detalles del mensaje de error y del código de error. Es posible que la solicitud no haya tenido éxito.	Cliente S3	"S3SL: Solicitud de selección de S3"

Código	Descripción	Utilizado por	Ver
SGET	S3 GET: registra una transacción exitosa para recuperar un objeto o enumerar los objetos en un depósito. **Nota:** Si la transacción opera en un subrecurso, el mensaje de auditoría incluirá el campo S3SR.	Cliente S3	"SGET: S3 OBTENER"
KARITÉ	S3 HEAD: Registra una transacción exitosa para verificar la existencia de un objeto o depósito.	Cliente S3	"SHEA: CABEZA T3"
WGET	Swift GET: registra una transacción exitosa para recuperar un objeto o enumerar los objetos en un contenedor.	Cliente Swift	"WGET: Obtención rápida"
TRIGO	Swift HEAD: registra una transacción exitosa para verificar la existencia de un objeto o contenedor.	Cliente Swift	"WHEA: CABEZA Veloz"

El cliente escribe mensajes de auditoría

Los mensajes de auditoría de escritura del cliente se registran cuando una aplicación cliente S3 realiza una solicitud para crear o modificar un objeto.

Código	Descripción	Utilizado por	Ver
OVWR	Sobrescritura de objeto: registra una transacción para sobrescribir un objeto con otro objeto.	Clientes S3 y Swift	"OVWR: Sobrescritura de objetos"
SDEL	S3 ELIMINAR: registra una transacción exitosa para eliminar un objeto o depósito. **Nota:** Si la transacción opera en un subrecurso, el mensaje de auditoría incluirá el campo S3SR.	Cliente S3	"SDEL: S3 ELIMINAR"
SPOS	S3 POST: registra una transacción exitosa para restaurar un objeto del almacenamiento de AWS Glacier a un grupo de almacenamiento en la nube.	Cliente S3	"SPOS: PUBLICACIÓN S3"
ESPOLVO	S3 PUT: Registra una transacción exitosa para crear un nuevo objeto o depósito. **Nota:** Si la transacción opera en un subrecurso, el mensaje de auditoría incluirá el campo S3SR.	Cliente S3	"SPUT: S3 PONER"
SUPD	Metadatos S3 actualizados: registra una transacción exitosa para actualizar los metadatos de un objeto o depósito existente.	Cliente S3	"SUPD: Metadatos S3 actualizados"

Código	Descripción	Utilizado por	Ver
WDEL	Swift DELETE: registra una transacción exitosa para eliminar un objeto o contenedor.	Cliente Swift	"WDEL: Eliminación rápida"
WPUT	Swift PUT: registra una transacción exitosa para crear un nuevo objeto o contenedor.	Cliente Swift	"WPUT: PUT rápido"

Mensaje de auditoría de gestión

La categoría Administración registra las solicitudes de los usuarios a la API de Administración.

Código	Título y descripción del mensaje	Ver
Universidad Estatal de Michigan	Mensaje de auditoría de la API de administración: un registro de solicitudes de usuario.	"MGAU: Mensaje de auditoría de gestión"

Mensajes de auditoría de ILM

Los mensajes de auditoría que pertenecen a la categoría de auditoría ILM se utilizan para eventos relacionados con las operaciones de gestión del ciclo de vida de la información (ILM).

Código	Título y descripción del mensaje	Ver
IDEL	Eliminación iniciada por ILM: este mensaje de auditoría se genera cuando ILM inicia el proceso de eliminación de un objeto.	"IDEL: Eliminación iniciada por ILM"
LKCU	Limpieza de objetos sobrescritos. Este mensaje de auditoría se genera cuando un objeto sobrescrito se elimina automáticamente para liberar espacio de almacenamiento.	"LKCU: Limpieza de objetos sobrescritos"
ORLM	Reglas de objeto cumplidas: este mensaje de auditoría se genera cuando los datos del objeto se almacenan según lo especificado por las reglas de ILM.	"ORLM: Se cumplen las reglas de objeto"

Referencia del mensaje de auditoría

BROR: Solicitud de solo lectura de depósito

El servicio LDR genera este mensaje de auditoría cuando un depósito entra o sale del modo de solo lectura. Por ejemplo, un depósito entra en modo de solo lectura mientras se eliminan todos los objetos.

Código	Campo	Descripción
BKHD	UUID del depósito	El identificador del depósito.
Brov	Valor de solicitud de solo lectura del depósito	Si el depósito se está convirtiendo en de solo lectura o está abandonando el estado de solo lectura (1 = solo lectura, 0 = no de solo lectura).
Hermanos	Razón de solo lectura del bucket	El motivo por el cual el depósito se convierte en de solo lectura o abandona ese estado. Por ejemplo, emptyBucket.
S3AI	ID de cuenta de inquilino de S3	El ID de la cuenta del inquilino que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.

CBRB: Inicio de recepción de objetos

Durante las operaciones normales del sistema, los bloques de contenido se transfieren continuamente entre diferentes nodos a medida que se accede a los datos, se replican y se conservan. Cuando se inicia la transferencia de un bloque de contenido de un nodo a otro, la entidad de destino emite este mensaje.

Código	Campo	Descripción
CNID	Identificador de conexión	El identificador único de la sesión/conexión de nodo a nodo.
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido que se está transfiriendo.
CTDR	Dirección de transferencia	Indica si la transferencia de CBID se inició mediante inserción o extracción: PUSH: La operación de transferencia fue solicitada por la entidad remitente. PULL: La operación de transferencia fue solicitada por la entidad receptora.
CTSR	Entidad de origen	El ID del nodo de la fuente (remitente) de la transferencia CBID.
CTDS	Entidad de destino	El ID del nodo del destino (receptor) de la transferencia CBID.

Código	Campo	Descripción
CTSS	Iniciar recuento de secuencias	Indica el primer recuento de secuencia solicitado. Si tiene éxito, la transferencia comienza a partir de este recuento de secuencia.
CTES	Recuento esperado de secuencia final	Indica el último recuento de secuencia solicitado. Si es exitosa, la transferencia se considera completa cuando se haya recibido este recuento de secuencia.
RSLT	Estado de inicio de la transferencia	Estado en el momento en que se inició la transferencia: SUCS: Transferencia iniciada exitosamente.

Este mensaje de auditoría significa que se inició una operación de transferencia de datos de nodo a nodo en una sola pieza de contenido, según lo identificado por su Identificador de bloque de contenido. La operación solicita datos desde "Recuento de secuencia inicial" hasta "Recuento de secuencia final esperado". Los nodos de envío y recepción se identifican mediante sus ID de nodo. Esta información se puede utilizar para rastrear el flujo de datos del sistema y, cuando se combina con mensajes de auditoría de almacenamiento, para verificar los recuentos de réplicas.

CBRE: Extremo de recepción de objetos

Cuando se completa la transferencia de un bloque de contenido de un nodo a otro, la entidad de destino emite este mensaje.

Código	Campo	Descripción
CNID	Identificador de conexión	El identificador único de la sesión/conexión de nodo a nodo.
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido que se está transfiriendo.
CTDR	Dirección de transferencia	Indica si la transferencia de CBID se inició mediante inserción o extracción: PUSH: La operación de transferencia fue solicitada por la entidad remitente. PULL: La operación de transferencia fue solicitada por la entidad receptora.
CTSR	Entidad de origen	El ID del nodo de la fuente (remitente) de la transferencia CBID.
CTDS	Entidad de destino	El ID del nodo del destino (receptor) de la transferencia CBID.

Código	Campo	Descripción
CTSS	Iniciar recuento de secuencias	Indica el recuento de secuencia en el que se inició la transferencia.
CTAS	Recuento de secuencia final real	Indica el último recuento de secuencia transferido exitosamente. Si el recuento de secuencia final real es el mismo que el recuento de secuencia inicial y el resultado de la transferencia no fue exitoso, no se intercambiaron datos.
RSLT	Resultado de la transferencia	El resultado de la operación de transferencia (desde la perspectiva de la entidad remitente): SUCS: transferencia completada exitosamente; se enviaron todos los recuentos de secuencia solicitados. CONL: conexión perdida durante la transferencia CTMO: tiempo de conexión agotado durante el establecimiento o la transferencia UNRE: ID de nodo de destino inalcanzable CRPT: transferencia finalizada debido a la recepción de datos corruptos o inválidos

Este mensaje de auditoría significa que se completó una operación de transferencia de datos de nodo a nodo. Si el resultado de la transferencia fue exitoso, la operación transfirió datos de "Recuento de secuencia inicial" a "Recuento de secuencia final real". Los nodos de envío y recepción se identifican mediante sus ID de nodo. Esta información se puede utilizar para rastrear el flujo de datos del sistema y para localizar, tabular y analizar errores. Cuando se combina con mensajes de auditoría de almacenamiento, también se puede utilizar para verificar los recuentos de réplicas.

CBSB: Inicio de envío de objetos

Durante las operaciones normales del sistema, los bloques de contenido se transfieren continuamente entre diferentes nodos a medida que se accede a los datos, se replican y se conservan. Cuando se inicia la transferencia de un bloque de contenido de un nodo a otro, la entidad de origen emite este mensaje.

Código	Campo	Descripción
CNID	Identificador de conexión	El identificador único de la sesión/conexión de nodo a nodo.
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido que se está transfiriendo.

Código	Campo	Descripción
CTDR	Dirección de transferencia	Indica si la transferencia de CBID se inició mediante inserción o extracción: PUSH: La operación de transferencia fue solicitada por la entidad remitente. PULL: La operación de transferencia fue solicitada por la entidad receptora.
CTSR	Entidad de origen	El ID del nodo de la fuente (remitente) de la transferencia CBID.
CTDS	Entidad de destino	El ID del nodo del destino (receptor) de la transferencia CBID.
CTSS	Iniciar recuento de secuencias	Indica el primer recuento de secuencia solicitado. Si tiene éxito, la transferencia comienza a partir de este recuento de secuencia.
CTES	Recuento esperado de secuencia final	Indica el último recuento de secuencia solicitado. Si es exitosa, la transferencia se considera completa cuando se haya recibido este recuento de secuencia.
RSLT	Estado de inicio de la transferencia	Estado en el momento en que se inició la transferencia: SUCS: transferencia iniciada exitosamente.

Este mensaje de auditoría significa que se inició una operación de transferencia de datos de nodo a nodo en una sola pieza de contenido, según lo identificado por su Identificador de bloque de contenido. La operación solicita datos desde "Recuento de secuencia inicial" hasta "Recuento de secuencia final esperado". Los nodos de envío y recepción se identifican mediante sus ID de nodo. Esta información se puede utilizar para rastrear el flujo de datos del sistema y, cuando se combina con mensajes de auditoría de almacenamiento, para verificar los recuentos de réplicas.

CBSE: Fin de envío de objetos

Cuando se completa la transferencia de un bloque de contenido de un nodo a otro, la entidad de origen emite este mensaje.

Código	Campo	Descripción
CNID	Identificador de conexión	El identificador único de la sesión/conexión de nodo a nodo.
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido que se está transfiriendo.

Código	Campo	Descripción
CTDR	Dirección de transferencia	Indica si la transferencia de CBID se inició mediante inserción o extracción: PUSH: La operación de transferencia fue solicitada por la entidad remitente. PULL: La operación de transferencia fue solicitada por la entidad receptora.
CTSR	Entidad de origen	El ID del nodo de la fuente (remitente) de la transferencia CBID.
CTDS	Entidad de destino	El ID del nodo del destino (receptor) de la transferencia CBID.
CTSS	Iniciar recuento de secuencias	Indica el recuento de secuencia en el que se inició la transferencia.
CTAS	Recuento de secuencia final real	Indica el último recuento de secuencia transferido exitosamente. Si el recuento de secuencia final real es el mismo que el recuento de secuencia inicial y el resultado de la transferencia no fue exitoso, no se intercambiaron datos.
RSLT	Resultado de la transferencia	El resultado de la operación de transferencia (desde la perspectiva de la entidad remitente): SUCS: Transferencia completada exitosamente; se enviaron todos los recuentos de secuencia solicitados. CONL: conexión perdida durante la transferencia CTMO: tiempo de conexión agotado durante el establecimiento o la transferencia UNRE: ID de nodo de destino inalcanzable CRPT: transferencia finalizada debido a la recepción de datos corruptos o inválidos

Este mensaje de auditoría significa que se completó una operación de transferencia de datos de nodo a nodo. Si el resultado de la transferencia fue exitoso, la operación transfirió datos de "Recuento de secuencia inicial" a "Recuento de secuencia final real". Los nodos de envío y recepción se identifican mediante sus ID de nodo. Esta información se puede utilizar para rastrear el flujo de datos del sistema y para localizar, tabular y analizar errores. Cuando se combina con mensajes de auditoría de almacenamiento, también se puede utilizar para verificar los recuentos de réplicas.

CGRR: Solicitud de replicación entre redes

Este mensaje se genera cuando StorageGRID intenta una operación de replicación entre

redes para replicar objetos entre depósitos en una conexión de federación de redes.

Código	Campo	Descripción
CSIZ	Tamaño del objeto	El tamaño del objeto en bytes. El atributo CSIZ se introdujo en StorageGRID 11.8. Como resultado, las solicitudes de replicación entre redes que abarcan una actualización de StorageGRID 11.7 a 11.8 podrían tener un tamaño de objeto total inexacto.
S3AI	ID de cuenta de inquilino de S3	El ID de la cuenta de inquilino que posee el depósito desde el que se está replicando el objeto.
GFID	ID de conexión de la federación de red	El ID de la conexión de federación de red que se utiliza para la replicación entre redes.
ÓPERA	Operación de la CGR	El tipo de operación de replicación entre redes que se intentó: • 0 = Replicar objeto • 1 = Replicar objeto multiparte • 2 = Replicar marcador de eliminación
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito.
VSID	ID de versión	El ID de la versión de la versión específica de un objeto que se estaba replicando.
RSLT	Código de resultado	Devuelve un resultado exitoso (SUCS) o un error general (GERR).

EBDL: Eliminar depósito vacío

El escáner ILM eliminó un objeto en un depósito que está eliminando todos los objetos (realizando una operación de depósito vacío).

Código	Campo	Descripción
CSIZ	Tamaño del objeto	El tamaño del objeto en bytes.
CAMINO	Cubo/clave S3	El nombre del depósito S3 y el nombre de la clave S3.
SEGC	UUID del contenedor	UUID del contenedor del objeto segmentado. Este valor solo está disponible si el objeto está segmentado.

Código	Campo	Descripción
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
RSLT	Resultado de la operación de eliminación	El resultado de un evento, proceso o transacción. Si no es relevante para un mensaje, se utiliza NONE en lugar de SUCS para que el mensaje no se filtre accidentalmente.

EBKR: Solicitud de cubo vacío

Este mensaje indica que un usuario envió una solicitud para activar o desactivar el depósito vacío (es decir, para eliminar objetos del depósito o para dejar de eliminar objetos).

Código	Campo	Descripción
CONSTRUIR	UUID del depósito	El identificador del depósito.
EBJS	Configuración JSON de depósito vacío	Contiene el JSON que representa la configuración actual del depósito vacío.
S3AI	ID de cuenta de inquilino de S3	El ID de la cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.

ECMC: Fragmento de datos con código de borrado faltante

Este mensaje de auditoría indica que el sistema ha detectado un fragmento de datos con código de borrado faltante.

Código	Campo	Descripción
VCMC	Identificación de VCS	El nombre del VCS que contiene el fragmento faltante.
MCID	Identificación del fragmento	El identificador del fragmento codificado por borrado que falta.
RSLT	Resultado	Este campo tiene el valor 'NINGUNO'. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje en particular. Se utiliza 'NONE' en lugar de 'SUCS' para que este mensaje no se filtre.

ECOC: Fragmento de datos corruptos codificados por borrado

Este mensaje de auditoría indica que el sistema ha detectado un fragmento de datos codificado por borrado corrupto.

Código	Campo	Descripción
VCCO	Identificación de VCS	El nombre del VCS que contiene el fragmento dañado.
VLID	ID de volumen	El volumen RangeDB que contiene el fragmento codificado de borrado dañado.
CCID	Identificación del fragmento	El identificador del fragmento codificado de borrado corrupto.
RSLT	Resultado	Este campo tiene el valor 'NINGUNO'. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje en particular. Se utiliza 'NONE' en lugar de 'SUCS' para que este mensaje no se filtre.

ETAF: Falló la autenticación de seguridad

Este mensaje se genera cuando falla un intento de conexión mediante Seguridad de la capa de transporte (TLS).

Código	Campo	Descripción
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP en la que falló la autenticación.
RUIDO	Identidad del usuario	Un identificador dependiente del servicio que representa la identidad del usuario remoto.

Código	Campo	Descripción
RSLT	Código de motivo	La razón del fallo: SCNI: Error en el establecimiento de conexión segura. CERM: Falta el certificado. CERT: El certificado no era válido. CERE: El certificado ha expirado. CERR: El certificado fue revocado. CSGN: La firma del certificado no era válida. CSGU: Se desconoce el firmante del certificado. UCRM: Faltaban credenciales de usuario. UCRI: Las credenciales de usuario no eran válidas. UCRU: No se permitieron las credenciales de usuario. TOUT: Se agotó el tiempo de autenticación.

Cuando se establece una conexión a un servicio seguro que utiliza TLS, las credenciales de la entidad remota se verifican utilizando el perfil TLS y la lógica adicional incorporada al servicio. Si esta autenticación falla debido a certificados o credenciales no válidos, inesperados o no permitidos, se registra un mensaje de auditoría. Esto permite realizar consultas sobre intentos de acceso no autorizado y otros problemas de conexión relacionados con la seguridad.

El mensaje podría ser el resultado de una entidad remota que tiene una configuración incorrecta o de intentos de presentar credenciales no válidas o no permitidas al sistema. Este mensaje de auditoría debe ser monitoreado para detectar intentos de obtener acceso no autorizado al sistema.

GNRG: Registro GNDS

El servicio CMN genera este mensaje de auditoría cuando un servicio ha actualizado o registrado información sobre sí mismo en el sistema StorageGRID .

Código	Campo	Descripción
RSLT	Resultado	El resultado de la solicitud de actualización: • SUCS: Exitoso • SUNV: Servicio no disponible • GERR: Otro fracaso
GNID	Nodo ID	El ID del nodo del servicio que inició la solicitud de actualización.

Código	Campo	Descripción
GNTP	Tipo de dispositivo	El tipo de dispositivo del nodo de la red (por ejemplo, BLDR para un servicio LDR).
GNDV	Versión del modelo del dispositivo	La cadena que identifica la versión del modelo del dispositivo del nodo de la red en el paquete DMDL.
GNGP	Grupo	El grupo al que pertenece el nodo de la red (en el contexto de los costos de enlace y la clasificación de consultas de servicio).
GNIA	Dirección IP	La dirección IP del nodo de la red.

Este mensaje se genera cada vez que un nodo de la cuadrícula actualiza su entrada en el paquete de nodos de la cuadrícula.

GNUR: Anulación del registro de GNDS

El servicio CMN genera este mensaje de auditoría cuando un servicio no ha registrado información sobre sí mismo en el sistema StorageGRID .

Código	Campo	Descripción
RSLT	Resultado	El resultado de la solicitud de actualización: • SUCS: Exitoso • SUNV: Servicio no disponible • GERR: Otro fracaso
GNID	Nodo ID	El ID del nodo del servicio que inició la solicitud de actualización.

GTED: Tarea de cuadrícula finalizada

Este mensaje de auditoría indica que el servicio CMN ha terminado de procesar la tarea de cuadrícula especificada y ha movido la tarea a la tabla Histórica. Si el resultado es SUCS, ABRT o ROLF, habrá un mensaje de auditoría de tarea de cuadrícula iniciada correspondiente. Los demás resultados indican que el procesamiento de esta tarea de cuadrícula nunca comenzó.

Código	Campo	Descripción
TSID	ID de tarea	Este campo identifica de forma única una tarea de cuadrícula generada y permite administrarla durante su ciclo de vida. **Nota:** El ID de tarea se asigna en el momento en que se genera una tarea de cuadrícula, no en el momento en que se envía. Es posible que una tarea de cuadrícula determinada se envíe varias veces y, en este caso, el campo ID de tarea no es suficiente para vincular de forma única los mensajes de auditoría Enviado, Iniciado y Finalizado.
RSLT	Resultado	El resultado del estado final de la tarea de cuadrícula: • SUCS: La tarea de cuadrícula se completó exitosamente. • ABRT: La tarea de cuadrícula se finalizó sin un error de reversión. • ROLF: La tarea de la red se finalizó y no se pudo completar el proceso de reversión. • CANC: La tarea de cuadrícula fue cancelada por el usuario antes de iniciarse. • EXPR: La tarea de la cuadrícula expiró antes de iniciarse. • IVLD: La tarea de cuadrícula no era válida. • AUTORIZACIÓN: La tarea de cuadrícula no fue autorizada. • DUPL: La tarea de cuadrícula fue rechazada por ser duplicada.

GTST: Tarea de cuadrícula iniciada

Este mensaje de auditoría indica que el servicio CMN ha comenzado a procesar la tarea de cuadrícula especificada. El mensaje de auditoría sigue inmediatamente al mensaje de Tarea de cuadrícula enviada para las tareas de cuadrícula iniciadas por el servicio interno de Envío de tareas de cuadrícula y seleccionadas para activación automática. Para las tareas de cuadrícula enviadas a la tabla Pendientes, este mensaje se genera cuando el usuario inicia la tarea de cuadrícula.

Código	Campo	Descripción
TSID	ID de tarea	Este campo identifica de forma única una tarea de cuadrícula generada y permite administrar la tarea durante su ciclo de vida. **Nota:** El ID de tarea se asigna en el momento en que se genera una tarea de cuadrícula, no en el momento en que se envía. Es posible que una tarea de cuadrícula determinada se envíe varias veces y, en este caso, el campo ID de tarea no es suficiente para vincular de forma única los mensajes de auditoría Enviado, Iniciado y Finalizado.
RSLT	Resultado	El resultado. Este campo solo tiene un valor: • SUCS: La tarea de cuadrícula se inició exitosamente.

GTSU: Tarea de cuadrícula enviada

Este mensaje de auditoría indica que se ha enviado una tarea de red al servicio CMN.

Código	Campo	Descripción
TSID	ID de tarea	Identifica de forma única una tarea de cuadrícula generada y permite gestionarla a lo largo de su ciclo de vida. **Nota:** El ID de tarea se asigna en el momento en que se genera una tarea de cuadrícula, no en el momento en que se envía. Es posible que una tarea de cuadrícula determinada se envíe varias veces y, en este caso, el campo ID de tarea no es suficiente para vincular de forma única los mensajes de auditoría Enviado, Iniciado y Finalizado.
TTYP	Tipo de tarea	El tipo de tarea de cuadrícula.
TVER	Versión de la tarea	Un número que indica la versión de la tarea de cuadrícula.
TDSC	Descripción de la tarea	Una descripción legible por humanos de la tarea de la cuadrícula.
VATS	Válido después de la marca de tiempo	El momento más temprano (microsegundos UINT64 a partir del 1 de enero de 1970 - hora UNIX) en el que la tarea de cuadrícula es válida.
VBTS	Válido antes de la marca de tiempo	El último momento (microsegundos UINT64 a partir del 1 de enero de 1970 - hora UNIX) en el que la tarea de cuadrícula es válida.
TSRC	Fuente	La fuente de la tarea: • TXTB: La tarea de cuadrícula se envió a través del sistema StorageGRID como un bloque de texto firmado. • GRID: La tarea de cuadrícula se envió a través del Servicio de envío de tareas de cuadrícula interno.
ACTV	Tipo de activación	El tipo de activación: • AUTO: La tarea de cuadrícula fue enviada para activación automática. • PEND: La tarea de la cuadrícula se envió a la tabla pendiente. Esta es la única posibilidad para la fuente TXTB.
RSLT	Resultado	El resultado de la presentación: • SUCS: La tarea de cuadrícula se envió correctamente. • ERROR: La tarea se ha movido directamente a la tabla histórica.

IDEL: Eliminación iniciada por ILM

Este mensaje se genera cuando ILM inicia el proceso de eliminación de un objeto.

El mensaje IDEL se genera en cualquiera de estas situaciones:

- **Para objetos en depósitos S3 compatibles**: este mensaje se genera cuando ILM inicia el proceso de eliminación automática de un objeto porque su período de retención ha expirado (suponiendo que la configuración de eliminación automática está habilitada y la retención legal está desactivada).
- **Para objetos en depósitos S3 no compatibles**. Este mensaje se genera cuando ILM inicia el proceso de eliminación de un objeto porque no hay instrucciones de ubicación en las políticas ILM activas que se apliquen actualmente al objeto.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El CBID del objeto.
CMPA	Cumplimiento: Eliminación automática	Solo para objetos en depósitos S3 compatibles. 0 (falso) o 1 (verdadero), indica si un objeto compatible debe eliminarse automáticamente cuando finaliza su período de retención, a menos que el depósito esté bajo una retención legal.
CMPL	Cumplimiento: Retención legal	Solo para objetos en depósitos S3 compatibles. 0 (falso) o 1 (verdadero), indica si el depósito se encuentra actualmente bajo retención legal.
CMPR	Cumplimiento: Periodo de conservación	Solo para objetos en depósitos S3 compatibles. La duración del período de retención del objeto en minutos.
CTME	Cumplimiento: Tiempo de ingesta	Solo para objetos en depósitos S3 compatibles. El tiempo de ingesta del objeto. Puede agregar el período de retención en minutos a este valor para determinar cuándo se puede eliminar el objeto del depósito.
DMRK	Eliminar ID de versión del marcador	El ID de la versión del marcador de eliminación creado al eliminar un objeto de un depósito versionado. Las operaciones en depósitos no incluyen este campo.
CSIZ	Tamaño del contenido	El tamaño del objeto en bytes.

Código	Campo	Descripción
LOCS	Ubicaciones	La ubicación de almacenamiento de los datos de objetos dentro del sistema StorageGRID . El valor de LOCS es "" si el objeto no tiene ubicaciones (por ejemplo, ha sido eliminado). CLEC: para objetos con código de borrado, el ID del perfil de codificación de borrado y el ID del grupo de codificación de borrado que se aplica a los datos del objeto. CLDI: para objetos replicados, el ID del nodo LDR y el ID del volumen de la ubicación del objeto. CLNL: ID del nodo ARC de la ubicación del objeto si los datos del objeto están archivados.
CAMINO	Cubo/clave S3	El nombre del depósito S3 y el nombre de la clave S3.
RSLT	Resultado	El resultado de la operación ILM. SUCS: La operación ILM fue exitosa.
REGLA	Etiqueta de reglas	• Si un objeto en un bucket S3 compatible se elimina automáticamente porque su período de retención ha expirado, este campo estará en blanco. • Si se elimina el objeto porque no hay más instrucciones de ubicación que se apliquen actualmente al objeto, este campo muestra la etiqueta legible por humanos de la última regla ILM que se aplicó al objeto.
SGRP	Sitio (Grupo)	Si está presente, el objeto se eliminó en el sitio especificado, que no es el sitio donde se ingirió el objeto.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de la versión específica de un objeto que se eliminó. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.

LKCU: Limpieza de objetos sobrescritos

Este mensaje se genera cuando StorageGRID elimina un objeto sobrescrito que anteriormente requería limpieza para liberar espacio de almacenamiento. Un objeto se sobrescribe cuando un cliente S3 escribe un objeto en una ruta que ya contiene un objeto. El proceso de eliminación se produce de forma automática y en segundo plano.

Código	Campo	Descripción
CSIZ	Tamaño del contenido	El tamaño del objeto en bytes.
LTYP	Tipo de limpieza	*Sólo para uso interno.*
LUID	UUID del objeto eliminado	El identificador del objeto que fue eliminado.
CAMINO	Cubo/clave S3	El nombre del depósito S3 y el nombre de la clave S3.
SEGC	UUID del contenedor	UUID del contenedor del objeto segmentado. Este valor solo está disponible si el objeto está segmentado.
UUID	Identificador único universal	El identificador del objeto que todavía existe. Este valor solo está disponible si el objeto no ha sido eliminado.

LKDM: Limpieza de objetos filtrados

Este mensaje se genera cuando se ha limpiado o eliminado un fragmento filtrado. Un fragmento puede ser parte de un objeto replicado o de un objeto codificado para borrado.

Código	Campo	Descripción
CLOC	Ubicación del fragmento	La ruta del archivo del fragmento filtrado que se eliminó.

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

Código	Campo	Descripción

LTYP	Tipo de fuga	Los cinco tipos de fugas que se pueden detectar:
		
		`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	Tiempo de creación de fragmentos	Hora en que se creó el fragmento filtrado.
UUID	Identificador único universal	El identificador del objeto al que pertenece el fragmento.
CBD	Identificador de bloque de contenido	CBID del objeto al que pertenece el fragmento filtrado.
CSIZ	Tamaño del contenido	El tamaño del fragmento en bytes.

LLST: Ubicación perdida

Este mensaje se genera siempre que no se puede encontrar una ubicación para una copia de un objeto (replicada o codificada por borrado).

Código	Campo	Descripción
CBIL	CBD	El CBD afectado.
ECPR	Perfil de codificación de borrado	Para datos de objetos codificados por borrado. El ID del perfil de codificación de borrado utilizado.

Código	Campo	Descripción
LTYP	Tipo de ubicación	CLDI (en línea): para datos de objetos replicados CLEC (en línea): para datos de objetos codificados por borrado CLNL (Nearline): para datos de objetos replicados archivados
NOID	ID del nodo de origen	El ID del nodo en el que se perdieron las ubicaciones.
PCLD	Ruta al objeto replicado	La ruta completa a la ubicación del disco de los datos del objeto perdido. Sólo se devuelve cuando LTYP tiene un valor de CLDI (es decir, para objetos replicados). Toma la forma `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Resultado	Siempre NINGUNO. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. Se utiliza NONE en lugar de SUCS para que este mensaje no se filtre.
TSRC	Fuente de activación	USUARIO: Usuario activado SYST: Sistema activado
UUID	Identificación universalmente única	El identificador del objeto afectado en el sistema StorageGRID .

MGAU: Mensaje de auditoría de gestión

La categoría Administración registra las solicitudes de los usuarios a la API de Administración. Cada solicitud HTTP que no sea una solicitud GET o HEAD a una URI de API válida registra una respuesta que contiene el nombre de usuario, la IP y el tipo de solicitud a la API. Las URI de API no válidas (como /api/v3-authorize) y las solicitudes no válidas a URI de API válidas no se registran.

Código	Campo	Descripción
MDIP	Dirección IP de destino	La dirección IP del servidor (destino).
ADNmd	Nombre de dominio	El nombre de dominio del host.
MPAT	Solicitar PATH	La ruta de la solicitud.

Código	Campo	Descripción
MPQP	Parámetros de consulta de solicitud	Los parámetros de consulta para la solicitud.
MRBD	Cuerpo de la solicitud	El contenido del cuerpo de la solicitud. Si bien el cuerpo de la respuesta se registra de forma predeterminada, el cuerpo de la solicitud se registra en ciertos casos cuando el cuerpo de la respuesta está vacío. Como la siguiente información no está disponible en el cuerpo de la respuesta, se toma del cuerpo de la solicitud para los siguientes métodos POST: • Nombre de usuario e ID de cuenta en **POST autorizar** • Nueva configuración de subredes en **POST /grid/grid-networks/update** • Nuevos servidores NTP en **POST /grid/ntp-servers/update** • ID de servidores dados de baja en **POST /grid/servers/decommission** **Nota:** La información confidencial se elimina (por ejemplo, una clave de acceso S3) o se oculta con asteriscos (por ejemplo, una contraseña).
MRMD	Método de solicitud	El método de solicitud HTTP: • CORREO • PONER • BORRAR • PARCHE
MRSC	Código de respuesta	El código de respuesta.
Precio de venta sugerido al público	Cuerpo de la respuesta	El contenido de la respuesta (el cuerpo de la respuesta) se registra de forma predeterminada. **Nota:** La información confidencial se elimina (por ejemplo, una clave de acceso S3) o se oculta con asteriscos (por ejemplo, una contraseña).
MSIP	Dirección IP de origen	La dirección IP del cliente (fuente).
MUUN	URN de usuario	El URN (nombre uniforme del recurso) del usuario que envió la solicitud.
RSLT	Resultado	Devuelve el éxito (SUCS) o el error informado por el backend.

OLST: El sistema detectó un objeto perdido

Este mensaje se genera cuando el servicio DDS no puede localizar ninguna copia de un

objeto dentro del sistema StorageGRID .

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El CBID del objeto perdido.
NOID	Nodo ID	Si está disponible, la última ubicación conocida, directa o cercana, del objeto perdido. Es posible tener solo el ID de nodo sin un ID de volumen si la información del volumen no está disponible.
CAMINO	Cubo/clave S3	Si está disponible, el nombre del depósito S3 y el nombre de la clave S3.
RSLT	Resultado	Este campo tiene el valor NINGUNO. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. Se utiliza NONE en lugar de SUCS para que este mensaje no se filtre.
UUID	Identificación universalmente única	El identificador del objeto perdido dentro del sistema StorageGRID .
VOLI	ID de volumen	Si está disponible, el ID de volumen del nodo de almacenamiento de la última ubicación conocida del objeto perdido.

ORLM: Se cumplen las reglas de objeto

Este mensaje se genera cuando el objeto se almacena y copia correctamente según lo especificado por las reglas de ILM.

> El mensaje ORLM no se genera cuando un objeto se almacena correctamente mediante la regla predeterminada Hacer 2 copias si otra regla en la política utiliza el filtro avanzado Tamaño del objeto.

Código	Campo	Descripción
CONSTRUIR	Encabezado del cubo	Campo de identificación del depósito. Se utiliza para operaciones internas. Sólo aparece si STAT es PRGD.
CBD	Identificador de bloque de contenido	El CBID del objeto.
CSIZ	Tamaño del contenido	El tamaño del objeto en bytes.

Código	Campo	Descripción
LOCS	Ubicaciones	La ubicación de almacenamiento de los datos de objetos dentro del sistema StorageGRID . El valor de LOCS es "" si el objeto no tiene ubicaciones (por ejemplo, ha sido eliminado). CLEC: para objetos con código de borrado, el ID del perfil de codificación de borrado y el ID del grupo de codificación de borrado que se aplica a los datos del objeto. CLDI: para objetos replicados, el ID del nodo LDR y el ID del volumen de la ubicación del objeto. CLNL: ID del nodo ARC de la ubicación del objeto si los datos del objeto están archivados.
CAMINO	Cubo/clave S3	El nombre del depósito S3 y el nombre de la clave S3.
RSLT	Resultado	El resultado de la operación ILM. SUCS: La operación ILM fue exitosa.
REGLA	Etiqueta de reglas	La etiqueta legible por humanos dada a la regla ILM aplicada a este objeto.
SEGC	UUID del contenedor	UUID del contenedor del objeto segmentado. Este valor solo está disponible si el objeto está segmentado.
SGCB	Contenedor CBDI	CBID del contenedor del objeto segmentado. Este valor solo está disponible para objetos segmentados y multiparte.
ESTADÍSTICA	Estado	El estado de la operación de ILM. HECHO: Se han completado las operaciones ILM contra el objeto. DFER: El objeto ha sido marcado para una futura reevaluación ILM. PRGD: El objeto ha sido eliminado del sistema StorageGRID . NLOC: Los datos del objeto ya no se pueden encontrar en el sistema StorageGRID . Este estado podría indicar que todas las copias de los datos del objeto faltan o están dañadas.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de un nuevo objeto creado en un depósito versionado. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.

El mensaje de auditoría ORLM se puede emitir más de una vez para un solo objeto. Por ejemplo, se emite

siempre que ocurre uno de los siguientes eventos:

- Las reglas ILM para el objeto se satisfacen para siempre.
- Las reglas ILM para el objeto se cumplen para esta época.
- Las reglas de ILM han eliminado el objeto.
- El proceso de verificación de fondo detecta que una copia de los datos del objeto replicado está dañada. El sistema StorageGRID realiza una evaluación ILM para reemplazar el objeto dañado.

Información relacionada

- "Transacciones de ingesta de objetos"
- "Transacciones de eliminación de objetos"

OVWR: Sobrescritura de objetos

Este mensaje se genera cuando una operación externa (solicitada por el cliente) hace que un objeto sea sobrescrito por otro objeto.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido (nuevo)	El CBID del nuevo objeto.
CSIZ	Tamaño del objeto anterior	El tamaño, en bytes, del objeto que se está sobrescribiendo.
Trastorno obsesivo-compulsivo (OCBD)	Identificador de bloque de contenido (anterior)	El CBID del objeto anterior.
UUID	Identificación única universal (nueva)	El identificador del nuevo objeto dentro del sistema StorageGRID .
OUID	Identificación única universal (anterior)	El identificador del objeto anterior dentro del sistema StorageGRID .
CAMINO	Ruta del objeto S3	La ruta del objeto S3 utilizada tanto para el objeto anterior como para el nuevo
RSLT	Código de resultado	Resultado de la transacción de sobrescritura de objeto. El resultado siempre es: SUCS: Exitoso

Código	Campo	Descripción
SGRP	Sitio (Grupo)	Si está presente, el objeto sobrescrito se eliminó en el sitio especificado, que no es el sitio donde se ingirió el objeto sobrescrito.

S3SL: Solicitud de selección de S3

Este mensaje registra una finalización después de que se haya devuelto una solicitud S3 Select al cliente. El mensaje S3SL puede incluir detalles del mensaje de error y del código de error. Es posible que la solicitud no haya tenido éxito.

Código	Campo	Descripción
BYSC	Bytes escaneados	Número de bytes escaneados (recibidos) desde los nodos de almacenamiento. Es probable que BYSC y BYPR sean diferentes si el objeto está comprimido. Si el objeto está comprimido, BYSC tendrá el recuento de bytes comprimidos y BYPR serán los bytes después de la descompresión.
BYPR	Bytes procesados	Número de bytes procesados. Indica cuántos bytes de "Bytes escaneados" fueron realmente procesados o procesados por un trabajo S3 Select.
BYRT	Bytes devueltos	Número de bytes que un trabajo S3 Select devolvió al cliente.
REPR	Registros procesados	Número de registros o filas que un trabajo S3 Select recibió de los nodos de almacenamiento.
RERT	Registros devueltos	Número de registros o filas que un trabajo S3 Select devolvió al cliente.
JOFI	Trabajo terminado	Indica si el trabajo S3 Select finalizó el procesamiento o no. Si esto es falso, entonces el trabajo no pudo finalizar y los campos de error probablemente contendrán datos. Es posible que el cliente haya recibido resultados parciales o ningún resultado.
REID	ID de solicitud	Identificador de la solicitud S3 Select.
EXTRA	Tiempo de ejecución	El tiempo, en segundos, que tardó el trabajo de selección S3 en completarse.
ERMG	Mensaje de error	Mensaje de error que generó el trabajo S3 Select.
TERRENO	Tipo de error	Tipo de error que generó el trabajo S3 Select.

Código	Campo	Descripción
ANTE TODO	Seguimiento de errores	Seguimiento de pila de errores que generó el trabajo S3 Select.
S3BK	Cubo S3	El nombre del depósito S3.
S3AK	ID de clave de acceso S3 (remitente de la solicitud)	El ID de la clave de acceso S3 del usuario que envió la solicitud.
S3AI	ID de cuenta de inquilino de S3 (remitente de la solicitud)	El ID de la cuenta de inquilino del usuario que envió la solicitud.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito.

SADD: Desactivación de auditoría de seguridad

Este mensaje indica que el servicio de origen (ID de nodo) ha desactivado el registro de mensajes de auditoría; los mensajes de auditoría ya no se recopilan ni se envían.

Código	Campo	Descripción
AETM	Habilitar método	El método utilizado para deshabilitar la auditoría.
AEUN	Nombre de usuario	El nombre de usuario que ejecutó el comando para deshabilitar el registro de auditoría.
RSLT	Resultado	Este campo tiene el valor NINGUNO. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. Se utiliza NONE en lugar de SUCS para que este mensaje no se filtre.

El mensaje implica que el registro estaba habilitado anteriormente, pero ahora se ha deshabilitado. Normalmente esto se usa solo durante la ingesta masiva para mejorar el rendimiento del sistema. Luego de la actividad masiva, se restablece la auditoría (SADE) y la capacidad de deshabilitarla se bloquea de forma permanente.

SADE: Habilitación de auditoría de seguridad

Este mensaje indica que el servicio de origen (ID de nodo) ha restaurado el registro de mensajes de auditoría; los mensajes de auditoría se están recopilando y entregando nuevamente.

Código	Campo	Descripción
AETM	Habilitar método	El método utilizado para permitir la auditoría.
AEUN	Nombre de usuario	El nombre de usuario que ejecutó el comando para habilitar el registro de auditoría.
RSLT	Resultado	Este campo tiene el valor NINGUNO. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. Se utiliza NONE en lugar de SUCS para que este mensaje no se filtre.

El mensaje implica que el registro estaba previamente deshabilitado (SADD), pero ahora ha sido restaurado. Normalmente esto solo se utiliza durante la ingesta masiva para mejorar el rendimiento del sistema. Luego de la actividad masiva, se restablece la auditoría y la capacidad de deshabilitarla se bloquea de forma permanente.

SCMT: Confirmación del almacén de objetos

El contenido de la red no se pone a disposición ni se reconoce como almacenado hasta que se haya confirmado (lo que significa que se ha almacenado de forma persistente). El contenido almacenado de forma persistente se ha escrito completamente en el disco y ha pasado las comprobaciones de integridad relacionadas. Este mensaje se emite cuando un bloque de contenido se envía al almacenamiento.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido destinado al almacenamiento permanente.
RSLT	Código de resultado	Estado en el momento en que el objeto se almacenó en el disco: SUCS: Objeto almacenado exitosamente.

Este mensaje significa que un bloque de contenido determinado se ha almacenado y verificado por completo y ahora se puede solicitar. Se puede utilizar para rastrear el flujo de datos dentro del sistema.

SDEL: S3 ELIMINAR

Cuando un cliente S3 emite una transacción DELETE, se realiza una solicitud para eliminar el objeto o depósito especificado, o para eliminar un subrecurso de depósito/objeto. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones en depósitos no incluyen este campo.

Código	Campo	Descripción
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP Consistency-Control, si está presente en la solicitud.
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño del contenido	El tamaño del objeto eliminado en bytes. Las operaciones en depósitos no incluyen este campo.
DMRK	Eliminar ID de versión del marcador	El ID de la versión del marcador de eliminación creado al eliminar un objeto de un depósito versionado. Las operaciones en depósitos no incluyen este campo.
GFID	ID de conexión de la federación de red	El ID de conexión de la conexión de federación de red asociada con una solicitud de eliminación de replicación entre redes. Sólo se incluye en los registros de auditoría de la red de destino.
GFSA	ID de cuenta de origen de Grid Federation	El ID de cuenta del inquilino en la red de origen para una solicitud de eliminación de replicación entre redes. Sólo se incluye en los registros de auditoría de la red de destino.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For`se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP). `x-amz-bypass-governance-retention`Se incluye automáticamente si está presente en la solicitud.
MTME	Hora de última modificación	La marca de tiempo de Unix, en microsegundos, que indica cuándo se modificó el objeto por última vez.
RSLT	Código de resultado	Resultado de la transacción DELETE. El resultado siempre es: SUCS: Exitoso
S3AI	ID de cuenta de inquilino de S3 (remitente de la solicitud)	El ID de la cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.

Código	Campo	Descripción
S3AK	ID de clave de acceso S3 (remitente de la solicitud)	El ID de clave de acceso S3 en formato hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito. Las operaciones en depósitos no incluyen este campo.
S3SR	Subrecurso S3	El subrecurso del objeto o depósito en el que se opera, si corresponde.
SACC	Nombre de la cuenta del inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de inquilino del usuario que envió la solicitud. Vacío para solicitudes anónimas.
SAIP	Dirección IP (remitente de la solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de la cuenta del inquilino de S3 (propietario del depósito)	El nombre de la cuenta del inquilino del propietario del depósito. Se utiliza para identificar acceso entre cuentas o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del depósito)	El ID de la cuenta de inquilino del propietario del depósito de destino. Se utiliza para identificar acceso entre cuentas o anónimo.
SGRP	Sitio (Grupo)	Si está presente, el objeto se eliminó en el sitio especificado, que no es el sitio donde se ingirió el objeto.
SUSR	URN de usuario S3 (remitente de la solicitud)	El ID de la cuenta del inquilino y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: `urn:sgws:identity::03393893651506583485:root` Vacío para solicitudes anónimas.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.

Código	Campo	Descripción
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUDM	Identificador único universal para un marcador de eliminación	El identificador de un marcador de eliminación. Los mensajes del registro de auditoría especifican UUDM o UUID, donde UUDM indica un marcador de eliminación creado como resultado de una solicitud de eliminación de objeto y UUID indica un objeto.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de la versión específica de un objeto que se eliminó. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.

SGET: S3 OBTENER

Cuando un cliente S3 emite una transacción GET, se realiza una solicitud para recuperar un objeto o enumerar los objetos en un depósito, o para eliminar un subrecurso de depósito/objeto. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones en depósitos no incluyen este campo.
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP Consistency-Control, si está presente en la solicitud.
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño del contenido	El tamaño del objeto recuperado en bytes. Las operaciones en depósitos no incluyen este campo.

Código	Campo	Descripción
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For`se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
LIDAD	ListObjectsV2	Se solicitó una respuesta en formato *v2*. Para más detalles, consulte "AWS ListObjectsV2" . Solo para operaciones de depósito GET.
NCHD	Número de niños	Incluye claves y prefijos comunes. Solo para operaciones de depósito GET.
RANG	Rango de lectura	Solo para operaciones de lectura de rango. Indica el rango de bytes que se leyeron en esta solicitud. El valor después de la barra (/) muestra el tamaño del objeto completo.
RSLT	Código de resultado	Resultado de la transacción GET. El resultado siempre es: SUCS: Exitoso
S3AI	ID de cuenta de inquilino de S3 (remitente de la solicitud)	El ID de la cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de la solicitud)	El ID de clave de acceso S3 en formato hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito. Las operaciones en depósitos no incluyen este campo.
S3SR	Subrecurso S3	El subrecurso del objeto o depósito en el que se opera, si corresponde.
SACC	Nombre de la cuenta del inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de inquilino del usuario que envió la solicitud. Vacío para solicitudes anónimas.

Código	Campo	Descripción
SAIP	Dirección IP (remitente de la solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de la cuenta del inquilino de S3 (propietario del depósito)	El nombre de la cuenta del inquilino del propietario del depósito. Se utiliza para identificar acceso entre cuentas o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del depósito)	El ID de la cuenta de inquilino del propietario del depósito de destino. Se utiliza para identificar acceso entre cuentas o anónimo.
SUSR	URN de usuario S3 (remitente de la solicitud)	El ID de la cuenta del inquilino y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: `urn:sgws:identity::03393893651506583485:root` Vacío para solicitudes anónimas.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
República Turca del Norte de Tennessee	Truncado o no truncado	Establezca como falso si se devolvieron todos los resultados. Establezca como verdadero si hay más resultados disponibles para devolver. Solo para operaciones de depósito GET.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de la versión específica de un objeto que se solicitó. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.

SHEA: CABEZA T3

Cuando un cliente S3 emite una transacción HEAD, se realiza una solicitud para verificar la existencia de un objeto o depósito y recuperar los metadatos sobre un objeto. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones en depósitos no incluyen este campo.
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño del contenido	El tamaño del objeto comprobado en bytes. Las operaciones en depósitos no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For`se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
RSLT	Código de resultado	Resultado de la transacción GET. El resultado siempre es: SUCS: Exitoso
S3AI	ID de cuenta de inquilino de S3 (remitente de la solicitud)	El ID de la cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de la solicitud)	El ID de clave de acceso S3 en formato hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito. Las operaciones en depósitos no incluyen este campo.
SACC	Nombre de la cuenta del inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de inquilino del usuario que envió la solicitud. Vacío para solicitudes anónimas.

Código	Campo	Descripción
SAIP	Dirección IP (remitente de la solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de la cuenta del inquilino de S3 (propietario del depósito)	El nombre de la cuenta del inquilino del propietario del depósito. Se utiliza para identificar acceso entre cuentas o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del depósito)	El ID de la cuenta de inquilino del propietario del depósito de destino. Se utiliza para identificar acceso entre cuentas o anónimo.
SUSR	URN de usuario S3 (remitente de la solicitud)	El ID de la cuenta del inquilino y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: `urn:sgws:identity::03393893651506583485:root` Vacío para solicitudes anónimas.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de la versión específica de un objeto que se solicitó. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.

SPOS: PUBLICACIÓN S3

Cuando un cliente S3 emite una solicitud de objeto POST, el servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0.

Código	Campo	Descripción
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP Consistency-Control, si está presente en la solicitud.
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño del contenido	El tamaño del objeto recuperado en bytes.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For`se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP). (No esperado para SPOS).
RSLT	Código de resultado	Resultado de la solicitud RestoreObject. El resultado siempre es: SUCS: Exitoso
S3AI	ID de cuenta de inquilino de S3 (remitente de la solicitud)	El ID de la cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de la solicitud)	El ID de clave de acceso S3 en formato hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito. Las operaciones en depósitos no incluyen este campo.
S3SR	Subrecurso S3	El subrecurso del objeto o depósito en el que se opera, si corresponde. Establezca en "seleccionar" para una operación de selección S3.

Código	Campo	Descripción
SACC	Nombre de la cuenta del inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de inquilino del usuario que envió la solicitud. Vacío para solicitudes anónimas.
SAIP	Dirección IP (remitente de la solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de la cuenta del inquilino de S3 (propietario del depósito)	El nombre de la cuenta del inquilino del propietario del depósito. Se utiliza para identificar acceso entre cuentas o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del depósito)	El ID de la cuenta de inquilino del propietario del depósito de destino. Se utiliza para identificar acceso entre cuentas o anónimo.
SRCF	Configuración de subrecursos	Restaurar información.
SUSR	URN de usuario S3 (remitente de la solicitud)	El ID de la cuenta del inquilino y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: `urn:sgws:identity::03393893651506583485:root` Vacío para solicitudes anónimas.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de la versión específica de un objeto que se solicitó. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.

SPUT: S3 PONER

Cuando un cliente S3 emite una transacción PUT, se realiza una solicitud para crear un

nuevo objeto o depósito, o para eliminar un subrecurso de depósito/objeto. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones en depósitos no incluyen este campo.
CMPS	Configuración de cumplimiento	La configuración de cumplimiento utilizada al crear el depósito, si está presente en la solicitud (truncada a los primeros 1024 caracteres).
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP Consistency-Control, si está presente en la solicitud.
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño del contenido	El tamaño del objeto recuperado en bytes. Las operaciones en depósitos no incluyen este campo.
GFID	ID de conexión de la federación de red	El ID de conexión de la conexión de federación de red asociada con una solicitud PUT de replicación entre redes. Sólo se incluye en los registros de auditoría de la red de destino.
GFSA	ID de cuenta de origen de Grid Federation	El ID de cuenta del inquilino en la red de origen para una solicitud PUT de replicación entre redes. Sólo se incluye en los registros de auditoría de la red de destino.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For`se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP). `x-amz-bypass-governance-retention`Se incluye automáticamente si está presente en la solicitud.
LKEN	Bloqueo de objetos habilitado	Valor del encabezado de la solicitud `x-amz-bucket-object-lock-enabled` , si está presente en la solicitud.

Código	Campo	Descripción
LKLH	Bloqueo de objeto con retención legal	Valor del encabezado de la solicitud `x-amz-object-lock-legal-hold` , si está presente en la solicitud PutObject.
LKMD	Modo de retención de bloqueo de objetos	Valor del encabezado de la solicitud `x-amz-object-lock-mode` , si está presente en la solicitud PutObject.
LKRU	Bloqueo de objeto Retener hasta fecha	Valor del encabezado de la solicitud `x-amz-object-lock-retain-until-date` , si está presente en la solicitud PutObject. Los valores están limitados a los 100 años a partir de la fecha en que se ingirió el objeto.
MTME	Hora de última modificación	La marca de tiempo de Unix, en microsegundos, que indica cuándo se modificó el objeto por última vez.
RSLT	Código de resultado	Resultado de la transacción PUT. El resultado siempre es: SUCS: Exitoso
S3AI	ID de cuenta de inquilino de S3 (remitente de la solicitud)	El ID de la cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de la solicitud)	El ID de clave de acceso S3 en formato hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito. Las operaciones en depósitos no incluyen este campo.
S3SR	Subrecurso S3	El subrecurso del objeto o depósito en el que se opera, si corresponde.
SACC	Nombre de la cuenta del inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de inquilino del usuario que envió la solicitud. Vacío para solicitudes anónimas.
SAIP	Dirección IP (remitente de la solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.

Código	Campo	Descripción
SBAC	Nombre de la cuenta del inquilino de S3 (propietario del depósito)	El nombre de la cuenta del inquilino del propietario del depósito. Se utiliza para identificar acceso entre cuentas o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del depósito)	El ID de la cuenta de inquilino del propietario del depósito de destino. Se utiliza para identificar acceso entre cuentas o anónimo.
SRCF	Configuración de subrecursos	La nueva configuración del subrecurso (truncada a los primeros 1024 caracteres).
SUSR	URN de usuario S3 (remitente de la solicitud)	El ID de la cuenta del inquilino y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: `urn:sgws:identity::03393893651506583485:root` Vacío para solicitudes anónimas.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
ULID	Subir ID	Incluido solo en mensajes SPUT para operaciones CompleteMultipartUpload. Indica que todas las piezas se han cargado y ensamblado.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de un nuevo objeto creado en un depósito versionado. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.
VSST	Estado de versiones	El nuevo estado de versión de un bucket. Se utilizan dos estados: "habilitado" o "suspendido". Las operaciones sobre objetos no incluyen este campo.

SREM: Eliminar almacén de objetos

Este mensaje se emite cuando se elimina contenido del almacenamiento persistente y ya no es accesible a través de las API normales.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido eliminado del almacenamiento permanente.
RSLT	Código de resultado	Indica el resultado de las operaciones de eliminación de contenido. El único valor definido es: SUCS: Contenido eliminado del almacenamiento persistente

Este mensaje de auditoría significa que un bloque de contenido determinado se ha eliminado de un nodo y ya no se puede solicitar directamente. El mensaje se puede utilizar para rastrear el flujo de contenido eliminado dentro del sistema.

SUPD: Metadatos S3 actualizados

La API S3 genera este mensaje cuando un cliente S3 actualiza los metadatos de un objeto ingerido. El servidor emite el mensaje si la actualización de metadatos es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones en depósitos no incluyen este campo.
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP Consistency-Control, si está presente en la solicitud, al actualizar la configuración de cumplimiento de un depósito.
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño del contenido	El tamaño del objeto recuperado en bytes. Las operaciones en depósitos no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For`se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).

Código	Campo	Descripción
RSLT	Código de resultado	Resultado de la transacción GET. El resultado siempre es: SUCS: exitoso
S3AI	ID de cuenta de inquilino de S3 (remitente de la solicitud)	El ID de la cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de la solicitud)	El ID de clave de acceso S3 en formato hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito. Las operaciones en depósitos no incluyen este campo.
SACC	Nombre de la cuenta del inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de inquilino del usuario que envió la solicitud. Vacío para solicitudes anónimas.
SAIP	Dirección IP (remitente de la solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de la cuenta del inquilino de S3 (propietario del depósito)	El nombre de la cuenta del inquilino del propietario del depósito. Se utiliza para identificar acceso entre cuentas o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del depósito)	El ID de la cuenta de inquilino del propietario del depósito de destino. Se utiliza para identificar acceso entre cuentas o anónimo.
SUSR	URN de usuario S3 (remitente de la solicitud)	El ID de la cuenta del inquilino y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: `urn:sgws:identity::03393893651506583485:root` Vacío para solicitudes anónimas.

Código	Campo	Descripción
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de la versión específica de un objeto cuyos metadatos se actualizaron. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.

SVRF: Error en la verificación del almacén de objetos

Este mensaje se emite siempre que un bloque de contenido no pasa el proceso de verificación. Cada vez que se leen o escriben datos de un objeto replicado en un disco, se realizan varias verificaciones e integridad para garantizar que los datos enviados al usuario solicitante sean idénticos a los datos ingresados originalmente en el sistema. Si alguna de estas comprobaciones falla, el sistema pone automáticamente en cuarentena los datos del objeto replicado dañado para evitar que se recuperen nuevamente.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido que no pasó la verificación.
RSLT	Código de resultado	Tipo de error de verificación: CRCF: Error en la verificación de redundancia cíclica (CRC). HMAC: Error en la verificación del código de autenticación de mensajes basado en hash (HMAC). EHSH: Hash de contenido cifrado inesperado. PHSH: Hash de contenido original inesperado. SEQC: Secuencia de datos incorrecta en el disco. PERR: Estructura no válida del archivo de disco. DERR: Error de disco. FNAM: Nombre de archivo incorrecto.

Este mensaje debe ser monitoreado de cerca. Las fallas de verificación de contenido pueden indicar fallas de hardware inminentes.

Para determinar qué operación activó el mensaje, consulte el valor del campo AMID (ID del módulo). Por ejemplo, un valor SVFY indica que el mensaje fue generado por el módulo Storage Verifier, es decir, verificación en segundo plano, y STOR indica que el mensaje fue activado por la recuperación de contenido.

SVRU: Verificación de almacén de objetos desconocida

El componente de almacenamiento del servicio LDR escanea continuamente todas las copias de datos de objetos replicados en el almacén de objetos. Este mensaje se emite cuando se detecta una copia desconocida o inesperada de datos de objetos replicados en el almacén de objetos y se mueve al directorio de cuarentena.

Código	Campo	Descripción
FPTH	Ruta del archivo	La ruta del archivo de la copia del objeto inesperado.
RSLT	Resultado	Este campo tiene el valor 'NINGUNO'. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. Se utiliza 'NONE' en lugar de 'SUCS' para que este mensaje no se filtre.

El mensaje de auditoría SVRU: Object Store Verify Unknown debe monitorearse de cerca. Significa que se detectaron copias inesperadas de datos de objetos en el almacén de objetos. Esta situación debe investigarse inmediatamente para determinar cómo se crearon estas copias, ya que puede indicar fallas inminentes de hardware.

SYSD: Parada de nodo

Cuando un servicio se detiene correctamente, se genera este mensaje para indicar que se solicitó el apagado. Normalmente, este mensaje se envía solo después de un reinicio posterior, porque la cola de mensajes de auditoría no se borra antes del apagado. Busque el mensaje SYST, enviado al comienzo de la secuencia de apagado, si el servicio no se ha reiniciado.

Código	Campo	Descripción
RSLT	Apagado limpio	La naturaleza del cierre: SUCS: El sistema se apagó limpiamente.

El mensaje no indica si se está deteniendo el servidor host, solo el servicio de informes. El RSLT de un SYSD no puede indicar un apagado "sucio", porque el mensaje se genera únicamente mediante apagados "limpios".

SYST: Nodo deteniéndose

Cuando un servicio se detiene correctamente, se genera este mensaje para indicar que se solicitó el apagado y que el servicio ha iniciado su secuencia de apagado. SYST se

puede utilizar para determinar si se solicitó el apagado antes de reiniciar el servicio (a diferencia de SYSD, que normalmente se envía después de reiniciar el servicio).

Código	Campo	Descripción
RSLT	Apagado limpio	La naturaleza del cierre: SUCS: El sistema se apagó limpiamente.

El mensaje no indica si se está deteniendo el servidor host, solo el servicio de informes. El código RSLT de un mensaje SYST no puede indicar un apagado "sucio", porque el mensaje se genera únicamente mediante apagados "limpios".

SYSU: Inicio del nodo

Cuando se reinicia un servicio, se genera este mensaje para indicar si el apagado anterior fue limpio (ordenado) o desordenado (inesperado).

Código	Campo	Descripción
RSLT	Apagado limpio	La naturaleza del cierre: SUCS: El sistema se apagó limpiamente. DSDN: El sistema no se apagó limpiamente. VRGN: El sistema se inició por primera vez después de la instalación (o reinstalación) del servidor.

El mensaje no indica si se inició el servidor host, solo el servicio de informes. Este mensaje se puede utilizar para:

- Detectar discontinuidad en el registro de auditoría.
- Determinar si un servicio está fallando durante la operación (ya que la naturaleza distribuida del sistema StorageGRID puede enmascarar estas fallas). El Administrador de servidor reinicia automáticamente un servicio fallido.

WDEL: Eliminación rápida

Cuando un cliente Swift emite una transacción DELETE, se realiza una solicitud para eliminar el objeto o contenedor especificado. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones sobre contenedores no incluyen este campo.

Código	Campo	Descripción
CSIZ	Tamaño del contenido	El tamaño del objeto eliminado en bytes. Las operaciones sobre contenedores no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For`se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
MTME	Hora de última modificación	La marca de tiempo de Unix, en microsegundos, que indica cuándo se modificó el objeto por última vez.
RSLT	Código de resultado	Resultado de la transacción DELETE. El resultado siempre es: SUCS: Exitoso
SAIP	Dirección IP del cliente solicitante	La dirección IP de la aplicación cliente que realizó la solicitud.
SGRP	Sitio (Grupo)	Si está presente, el objeto se eliminó en el sitio especificado, que no es el sitio donde se ingirió el objeto.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
WACC	ID de cuenta Swift	El ID de cuenta único según lo especificado por el sistema StorageGRID .
WCON	Contenedor Swift	El nombre del contenedor Swift.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones sobre contenedores no incluyen este campo.

Código	Campo	Descripción
WUSR	Usuario de cuenta Swift	El nombre de usuario de la cuenta Swift que identifica de forma única al cliente que realiza la transacción.

WGET: Obtención rápida

Cuando un cliente Swift emite una transacción GET, se realiza una solicitud para recuperar un objeto, enumerar los objetos en un contenedor o enumerar los contenedores en una cuenta. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones sobre cuentas y contenedores no incluyen este campo.
CSIZ	Tamaño del contenido	El tamaño del objeto recuperado en bytes. Las operaciones sobre cuentas y contenedores no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For`se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
RSLT	Código de resultado	Resultado de la transacción GET. El resultado es siempre SUCS: exitoso
SAIP	Dirección IP del cliente solicitante	La dirección IP de la aplicación cliente que realizó la solicitud.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .

Código	Campo	Descripción
WACC	ID de cuenta Swift	El ID de cuenta único según lo especificado por el sistema StorageGRID .
WCON	Contenedor Swift	El nombre del contenedor Swift. Las operaciones sobre cuentas no incluyen este campo.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones sobre cuentas y contenedores no incluyen este campo.
WUSR	Usuario de cuenta Swift	El nombre de usuario de la cuenta Swift que identifica de forma única al cliente que realiza la transacción.

WHEA: CABEZA Veloz

Cuando un cliente Swift emite una transacción HEAD, se realiza una solicitud para verificar la existencia de una cuenta, un contenedor o un objeto y recuperar cualquier metadato relevante. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones sobre cuentas y contenedores no incluyen este campo.
CSIZ	Tamaño del contenido	El tamaño del objeto recuperado en bytes. Las operaciones sobre cuentas y contenedores no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For`se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
RSLT	Código de resultado	Resultado de la transacción HEAD. El resultado siempre es: SUCS: exitoso
SAIP	Dirección IP del cliente solicitante	La dirección IP de la aplicación cliente que realizó la solicitud.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.

Código	Campo	Descripción
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
WACC	ID de cuenta Swift	El ID de cuenta único según lo especificado por el sistema StorageGRID .
WCON	Contenedor Swift	El nombre del contenedor Swift. Las operaciones sobre cuentas no incluyen este campo.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones sobre cuentas y contenedores no incluyen este campo.
WUSR	Usuario de cuenta Swift	El nombre de usuario de la cuenta Swift que identifica de forma única al cliente que realiza la transacción.

WPUT: PUT rápido

Cuando un cliente Swift emite una transacción PUT, se realiza una solicitud para crear un nuevo objeto o contenedor. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones sobre contenedores no incluyen este campo.
CSIZ	Tamaño del contenido	El tamaño del objeto recuperado en bytes. Las operaciones sobre contenedores no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For`se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
MTME	Hora de última modificación	La marca de tiempo de Unix, en microsegundos, que indica cuándo se modificó el objeto por última vez.

Código	Campo	Descripción
RSLT	Código de resultado	Resultado de la transacción PUT. El resultado siempre es: SUCS: exitoso
SAIP	Dirección IP del cliente solicitante	La dirección IP de la aplicación cliente que realizó la solicitud.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
WACC	ID de cuenta Swift	El ID de cuenta único según lo especificado por el sistema StorageGRID .
WCON	Contenedor Swift	El nombre del contenedor Swift.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones sobre contenedores no incluyen este campo.
WUSR	Usuario de cuenta Swift	El nombre de usuario de la cuenta Swift que identifica de forma única al cliente que realiza la transacción.