



Revisar los registros de auditoría

StorageGRID 11.7

NetApp
April 12, 2024

Tabla de contenidos

- Revisar los registros de auditoría 1
 - Revisar registros de auditoría: Información general 1
 - Auditar el flujo y la retención de mensajes 1
 - Acceda al archivo de registro de auditoría 4
 - Rotación del archivo de registro de auditoría 5
 - Formato del archivo de registro de auditoría 5
 - Formato de mensaje de auditoría 19
 - Auditar los mensajes y el ciclo de vida del objeto 24
 - Auditar mensajes 31

Revisar los registros de auditoría

Revisar registros de auditoría: Información general

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

Estas instrucciones son para los administradores responsables de generar informes sobre la actividad y el uso del sistema que requieran analizar los mensajes de auditoría del sistema StorageGRID.

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

Para obtener información sobre la configuración de niveles de mensajes de auditoría y el uso de un servidor de syslog externo, consulte "[Configurar los mensajes de auditoría y los destinos de registro](#)".

Auditar el flujo y la retención de mensajes

Todos los servicios de StorageGRID generan mensajes de auditoría durante el funcionamiento normal del sistema. Debe comprender la forma en que estos mensajes de auditoría pasan por el sistema StorageGRID al `audit.log` archivo.

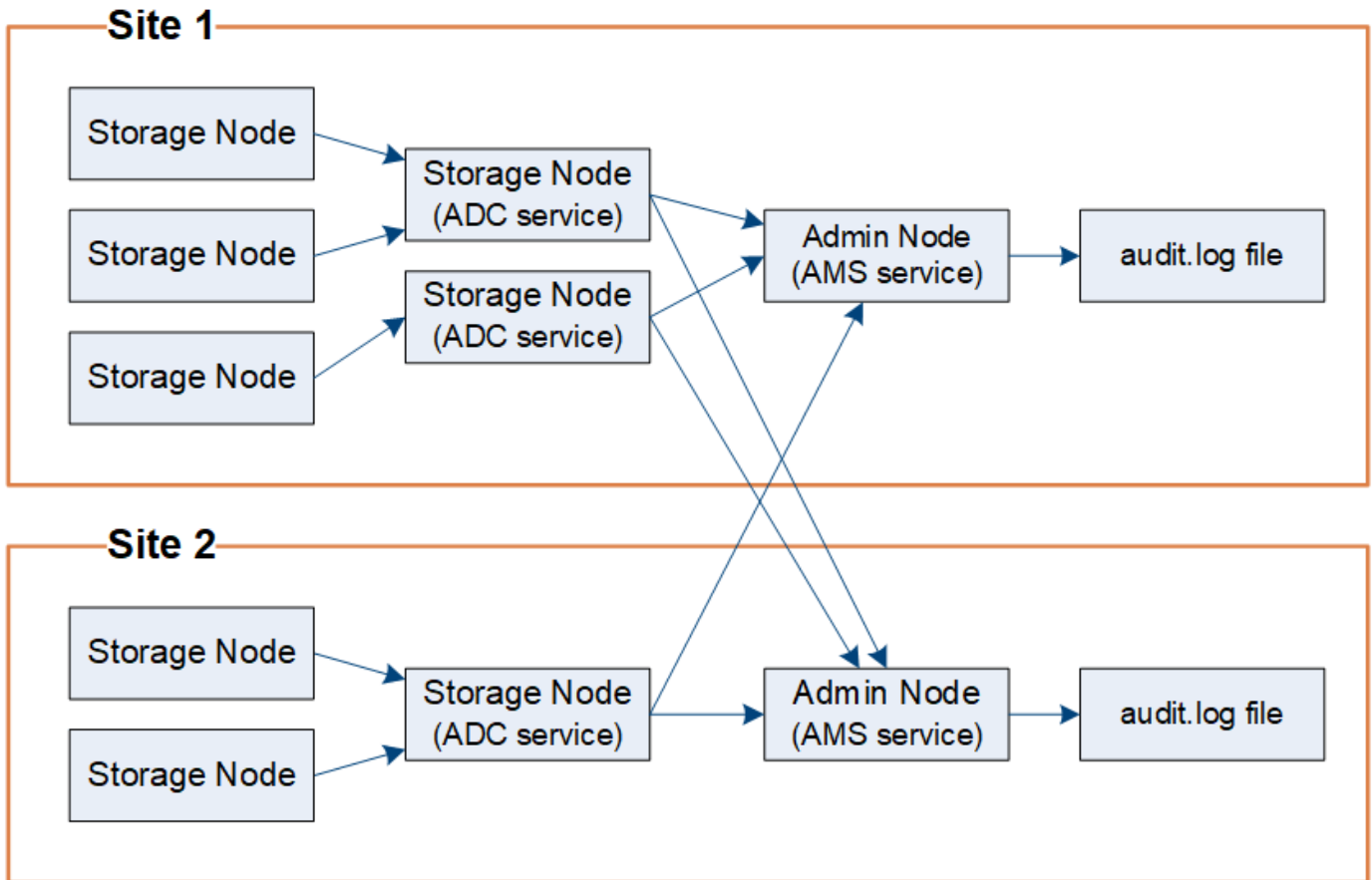
Flujo de mensajes de auditoría

Los mensajes de auditoría los procesan los nodos de administrador y los 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 del 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 relé y envía su colección de mensajes de auditoría a cada nodo de administración del sistema StorageGRID, lo que proporciona a cada nodo de administración un registro completo de la actividad del sistema.

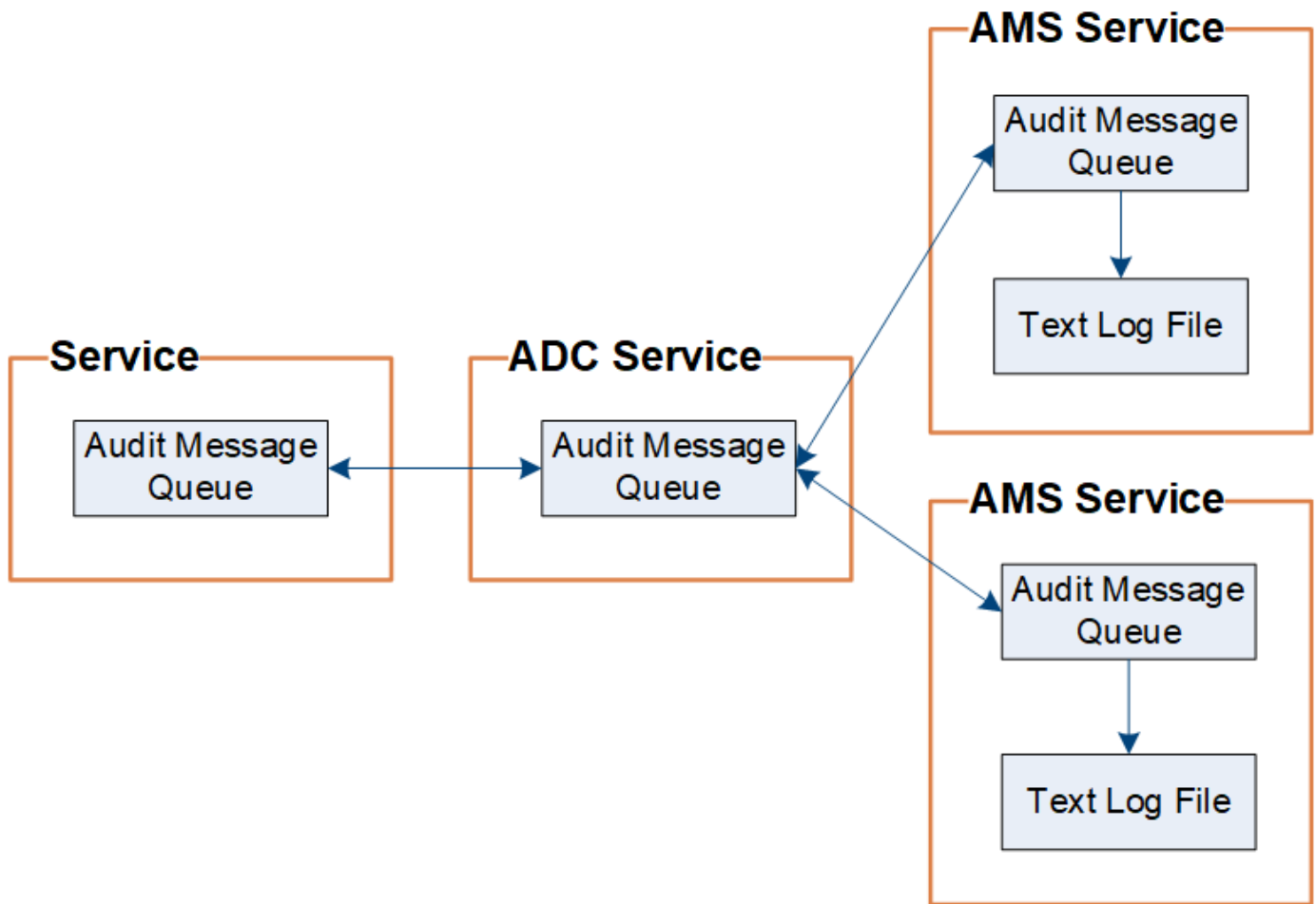
Cada nodo de administración almacena mensajes de auditoría en archivos de registro de texto; se asigna el nombre al archivo de registro activo `audit.log`.



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 transmite un mensaje de auditoría, el mensaje se almacena en una cola de mensajes de auditoría en el disco del sistema del nodo de cuadrícula. Siempre se mantiene una copia del mensaje en la cola de mensajes de auditoría hasta que el mensaje se escribe en el archivo de registro de auditoría del nodo de administración `/var/local/audit/export` 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 está demasiado lleno, los nodos individuales priorizarán el procesamiento de su acumulación y no estarán disponibles temporalmente para los mensajes nuevos.

Específicamente, puede ver los siguientes comportamientos:

- Si la `/var/local/audit/export` el directorio utilizado por un nodo de administración se llena, el nodo de administración se marcará como no disponible para los nuevos mensajes de auditoría hasta que el directorio ya no esté lleno. Las solicitudes de clientes S3 y Swift no se ven afectadas. La alarma XAMS (repositorios de auditoría no accesibles) se activa cuando no se puede acceder a un repositorio de auditoría.
- Si la `/var/local/` el directorio utilizado por un nodo de almacenamiento con el servicio ADC se llena al 92%, el nodo se marcará como no disponible para auditar mensajes hasta que el directorio sólo esté lleno al 87%. Las solicitudes de clientes de S3 y Swift a otros nodos no se ven afectadas. La alarma NRLY (Relés de auditoría disponibles) se activa cuando no se pueden acceder a los relés de auditoría.



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

- Si la `/var/local/` El directorio que utiliza un nodo de almacenamiento se llena al 85%, el nodo empezará a rechazar las solicitudes de cliente S3 y Swift `503 Service Unavailable`.

Los siguientes tipos de problemas pueden hacer que las colas de mensajes de auditoría crezcan muy grandes:

- La interrupción de un nodo de administrador o un nodo de almacenamiento con el servicio de ADC. Si uno de los nodos del sistema está inactivo, es posible que los nodos restantes se vuelvan a registrar.
- Tasa de actividad sostenida que supera la capacidad de auditoría del sistema.
- La `/var/local/` El espacio de un nodo de almacenamiento ADC se llena por motivos que no están relacionados con los mensajes de auditoría. Cuando esto sucede, el nodo deja de aceptar nuevos mensajes de auditoría y da prioridad a su acumulación actual, lo que puede provocar backlogs en otros nodos.

Alarma de alerta de cola de auditoría grande y mensajes de auditoría en cola (AMQS)

Para ayudarle a supervisar 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 el número de mensajes en una cola de nodos de almacenamiento o cola de nodos de administración alcanza determinados umbrales.

Si se activa la alerta **cola de auditoría grande** o la alarma AMQS heredada, comience comprobando la carga en el sistema—si ha habido un número significativo de transacciones recientes, la alerta y la alarma deben resolverse con el tiempo y pueden ignorarse.

Si la alerta o alarma persiste y aumenta su gravedad, vea un gráfico del tamaño de la cola. Si el número aumenta constantemente durante horas o días, es probable que la carga de auditoría haya superado la capacidad de auditoría del sistema. Reduzca la tasa de operaciones del cliente o disminuya el número de mensajes de auditoría registrados cambiando el nivel de auditoría de las escrituras del cliente y las lecturas del cliente a error o Desactivado. Consulte "[Configurar los mensajes de auditoría y los destinos de registro](#)".

Mensajes duplicados

El sistema StorageGRID toma un método conservador si se produce un fallo en la red o en un nodo. Por este motivo, puede haber mensajes duplicados en el registro de auditoría.

Acceda al archivo de registro de auditoría

El recurso compartido de auditoría contiene el activo `audit.log` archivo y todos los archivos de registro de auditoría comprimidos. Para facilitar el acceso a los registros de auditoría, usted podrá "[Configurar el acceso del cliente de auditoría para NFS](#)". También es posible acceder a los archivos del registro de auditoría directamente desde la línea de comandos del nodo de administración.

Antes de empezar

- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.
- Debe conocer la dirección IP de un nodo de administrador.

Pasos

1. Inicie sesión en un nodo de administrador:
 - a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

- c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
- d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

Cuando ha iniciado sesión como `root`, el símbolo del sistema cambia de `$` para `#`.

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

```
cd /var/local/audit/export
```

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

Rotación del archivo de registro de auditoría

Los archivos de registros de auditoría se guardan en un nodo administrador `/var/local/audit/export` directorio. Se denomina los archivos de registro de auditoría activos `audit.log`.



De manera opcional, se puede cambiar el destino de los registros de auditoría y enviar información de auditoría a un servidor de `syslog` externo. Se siguen generando y almacenando registros locales de registros de auditoría cuando se configura un servidor de `syslog` externo. Consulte "[Configurar los mensajes de auditoría y los destinos de registro](#)".

Una vez al día, el activo `audit.log` el archivo se guardará y se guardará un nuevo `audit.log` se ha iniciado el archivo. 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 los archivos utilizan la fecha en la que se guardó el archivo, añadido por un número, en formato `yyyy-mm-dd.txt.n`. Por ejemplo: `2018-04-15.txt` y `2018-04-15.txt.1` Son los primeros y segundos archivos de registro creados y guardados el 15 de abril de 2018.

Después de un día, el archivo guardado se comprime y cambia su nombre, en el formato `yyyy-mm-dd.txt.gz`, que conserva la fecha original. Con el tiempo, esto genera el consumo de almacenamiento asignado a los registros de auditoría en el nodo de administración. Una secuencia de comandos supervisa el consumo de espacio del registro de auditoría y elimina los archivos de registro según sea necesario para liberar espacio en la `/var/local/audit/export` directorio. Los registros de auditoría se eliminan según la fecha en la que se crearon, y la más antigua se eliminó primero. Puede supervisar las acciones del script en el siguiente archivo: `/var/local/log/manage-audit.log`.

En este ejemplo se muestra el activo `audit.log` archivo, el 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 del archivo de registro de auditoría

Formato de archivo de registro de auditoría: Información general

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

Cada mensaje de auditoría contiene lo siguiente:

- Hora universal coordinada (UTC) del evento que activó el mensaje de auditoría (ATIM) en formato ISO 8601, seguido de un espacio:

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

- El mensaje de auditoría mismo, entre corchetes y empezando por `AUDT`.

En el siguiente ejemplo se muestran tres mensajes de auditoría en un archivo de registro de auditoría (se han agregado saltos de línea para facilitar la lectura). Estos mensajes se generaron cuando un inquilino creó un bloque de S3 y se añadieron dos objetos a ese bloque.

2019-08-07T18:43:30.247711

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWnt-PhoTDwB9Jok7PtyLkQmA=="]  
[SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]  
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"]  
[AVER(UI32):10][ATIM(UI64):1565203410247711]  
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142142472611085]]
```

2019-08-07T18:43:30.783597

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWnt-PhoTDwB9Jok7PtyLkQmA=="]  
[SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]  
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"]  
[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(FC32):S3RQ][ATID(UI64):8439606722108456022]]
```

2019-08-07T18:43:30.784558

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWnt-PhoTDwB9Jok7PtyLkQmA=="]  
[SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]  
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"]  
[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(FC32):S3RQ][ATID(UI64):13489590586043706682]]
```

En su formato predeterminado, los mensajes de auditoría de los archivos de registro de auditoría no son fáciles de leer ni interpretar. Puede utilizar el [herramienta audit-explain](#) para obtener resúmenes simplificados de los mensajes de auditoría en el log de auditoría. Puede utilizar el [herramienta audit-sum](#) para resumir cuántas operaciones de escritura, lectura y eliminación se han registrado y cuánto tiempo demoraron estas operaciones.

Utilice la herramienta de explicación de auditoría

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

del registro de auditoría a un formato de fácil lectura.

Antes de empezar

- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.
- Debe conocer la dirección IP del nodo de administrador principal.

Acerca de esta tarea

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



La `audit-explain` herramienta está diseñada principalmente para su uso por parte del soporte técnico durante operaciones de solución de problemas. El procesamiento `audit-explain` Las consultas pueden consumir una gran cantidad de energía de CPU, lo que puede afectar a las operaciones de StorageGRID.

Este ejemplo muestra el resultado típico de `audit-explain` herramienta. Estos cuatro "SPUT" Los mensajes de auditoría se generaron cuando el inquilino de S3 con ID de cuenta 92484777680322627870 utilizó solicitudes PUT S3 para crear un bloque llamado «bucket1» y añadir tres objetos a ese bloque.

```
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
```

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

- Procesar registros de auditoría sin formato o comprimidos. Por ejemplo:

```
audit-explain audit.log
```

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

- Procese varios archivos simultáneamente. Por ejemplo:

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

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

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

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

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

Dado que los registros de auditoría pueden ser muy grandes y lentos de analizar, puede ahorrar tiempo filtrando las partes que desea ver y ejecutar `audit-explain` en las partes, en lugar del archivo completo.



La `audit-explain` herramienta no acepta archivos comprimidos como entrada con hilo. Para procesar archivos comprimidos, proporcione sus nombres de archivo como argumentos de línea de comandos o utilice `zcat` herramienta para descomprimir primero los archivos. Por ejemplo:

```
zcat audit.log.gz | audit-explain
```

Utilice la `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 `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
 - d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

Cuando ha iniciado sesión como `root`, el símbolo del sistema cambia de `$` para `#`.

2. Introduzca el comando siguiente, donde `/var/local/audit/export/audit.log` representa el nombre y la ubicación del archivo o archivos que desea analizar:

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

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



Para reducir las longitudes de línea y facilitar la lectura, las marcas de tiempo no se muestran por defecto. Si desea ver las marcas de tiempo, use la `Marca de hora (-t)` opción.

Utilice la herramienta de suma de auditoría

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

Antes de empezar

- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.
- Debe conocer la dirección IP del nodo de administrador principal.

Acerca de esta tarea

La `audit-sum` Herramienta, disponible en el nodo de administración principal, resume cuántas operaciones de escritura, lectura y eliminación se han registrado y cuánto tiempo han tardado estas operaciones.



La `audit-sum` la herramienta está diseñada principalmente para su uso por parte del soporte técnico durante operaciones de solución de problemas. Procesamiento `audit-sum` Las consultas pueden consumir una gran cantidad de energía de CPU, lo que puede afectar a las operaciones de StorageGRID.

Este ejemplo muestra el resultado típico de `audit-sum` herramienta. Este ejemplo muestra el tiempo que tardaban las operaciones de 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

```

La `audit-sum` La herramienta proporciona recuentos y horas para los siguientes mensajes de auditoría de S3, Swift y ILM en un registro de auditoría:

Codificación	Descripción	Consulta
ARCT	Archive recupere desde Cloud-Tier	"ARCT: Recuperación de archivos a partir de nivel de cloud"
ASCT	Almacenamiento de datos para el nivel cloud	"ASCT: Archive Store Cloud-Tier"
IDEL	ILM Initiated Delete: Registra cuando ILM inicia el proceso de eliminación de un objeto.	"IDEL: Eliminación de ILM iniciada"
SDEL	S3 DELETE: Registra una transacción realizada correctamente para eliminar un objeto o bloque.	"SDEL: ELIMINACIÓN DE S3"
SGET	S3 GET: Registra una transacción realizada correctamente para recuperar un objeto o enumerar los objetos de un bloque.	"SGET: S3 GET"

Codificación	Descripción	Consulte
SHEA	S3 HEAD: Registra una transacción realizada correctamente para comprobar la existencia de un objeto o bloque.	"SHEA: CABEZA S3"
SPUT	S3 PUT: Registra una transacción realizada correctamente para crear un nuevo objeto o bloque.	"SPUT: S3 PUT"
¡WDEL	Swift DELETE: Registra una transacción realizada correctamente para eliminar un objeto o un contenedor.	"WDEL: ELIMINACIÓN de Swift"
CONSIGA	Swift GET: Registra una transacción realizada correctamente para recuperar un objeto o enumerar los objetos de un contenedor.	"WGET: Swift GET"
WHEA	Swift HEAD: Registra una transacción realizada correctamente para comprobar la existencia de un objeto o contenedor.	"WHEA: CABEZA de Swift"
WPUT	Swift PUT: Registra una transacción correcta para crear un nuevo objeto o contenedor.	"WPUT: SWIFT PUT"

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

- Procesar registros de auditoría sin formato o comprimidos. Por ejemplo:

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

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

- Procese varios archivos simultáneamente. Por ejemplo:

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

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

- Acepte la entrada de una tubería, lo que le permite filtrar y preprocesar la entrada mediante 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 con hilo. Para procesar archivos comprimidos, proporcione sus nombres de archivo como argumentos de línea de comandos o utilice `zcat` herramienta para descomprimir primero los archivos. Por ejemplo:

```
audit-sum audit.log.gz

zcat audit.log.gz | audit-sum
```

Puede utilizar las opciones de línea de comandos para resumir las operaciones en bloques por separado de las operaciones en objetos o para agrupar resúmenes de mensajes por nombre de bloque, por período de tiempo o por tipo de destino. De forma predeterminada, los resúmenes muestran el tiempo mínimo, máximo y promedio de funcionamiento, pero puede utilizar `size (-s)` opción para mirar el tamaño del objeto en su lugar.

Utilice la `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 `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a la raíz: `su -`
 - d. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

Cuando ha iniciado sesión como `root`, el símbolo del sistema cambia de `$` para `#`.

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

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

Este ejemplo muestra el resultado típico de `audit-sum` herramienta. Este ejemplo muestra el tiempo que tardaban las operaciones de protocolo.

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
=====			
IDEL	274		
SDEL 0.352	213371	0.004	20.934
SGET 1.132	201906	0.010	1740.290
SHEA 0.272	22716	0.005	2.349
SPUT 0.487	1771398	0.011	1770.563

En este ejemplo, las operaciones SGET (S3 GET) son las más lentas en promedio a 1.13 segundos, pero las operaciones SGET y SPUT (S3 PUT) muestran tiempos largos en el peor de los casos de aproximadamente 1,770 segundos.

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

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

Los resultados incluyen el tipo (objeto o bloque) y la ruta de acceso, que le permite obtener el registro de auditoría de otros mensajes relacionados con estos objetos en particular.

```

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/r9010aQ8JB-1566861764-4519.iso
      1624414429    10.96.101.125    object    5375001556
backup/r9010aQ8JB-1566861764-6618.iso
      1533143793    10.96.101.125    object    5183661466
backup/r9010aQ8JB-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

```

+ Desde este ejemplo, puede ver que las tres solicitudes DE OBTENER S3 más lentas eran para objetos de un tamaño de 5 GB, mucho mayor que el de los otros objetos. El gran tamaño representa los lentos tiempos de recuperación en el peor de los casos.

3. Si desea determinar qué tamaños de objetos se están ingiriendo y recuperando de la cuadrícula, utilice la opción size (-s):

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


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

En este ejemplo, el tamaño medio del objeto para SPUT es inferior a 2.5 MB, pero el tamaño medio para SGET es mucho mayor. El número de mensajes SPUT es mucho mayor que el número de mensajes SGET, lo que indica que la mayoría de los objetos nunca se recuperan.

4. Si quieres determinar si las recuperaciones eran lentas ayer:
 - a. Emita el comando en el registro de auditoría correspondiente y use la opción group-by-Time (-gt), seguido del período de tiempo (por ejemplo, 15M, 1H, 10S):

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

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

Estos resultados muestran que S3 CONSIGUE tráfico pico entre 06:00 y 07:00. Los tiempos máximo y promedio son considerablemente más altos en estos tiempos también, y no subieron gradualmente a medida que el recuento aumentó. Esto sugiere que se ha superado la capacidad en algún lugar, quizás en la red o en la capacidad del grid para procesar solicitudes.

- b. Para determinar el tamaño de los objetos recuperados ayer cada hora, agregue la opción size (-s) para el mando:

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

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

Estos resultados indican que se han producido recuperaciones de gran tamaño cuando se alcanzó el máximo tráfico de recuperación total.

c. Para ver más detalles, utilice ["herramienta audit-explain"](#) 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 sea de muchas líneas, agregue 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 los segmentos son más lentas que las operaciones SPUT para los objetos:

a. Comience por utilizar el -go opción, que agrupa mensajes para operaciones de objeto y bloques por separado:

```
grep SPUT sample.log | audit-sum -go
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.bucket 0.125	1	0.125	0.125
SPUT.object 0.236	12	0.025	1.019

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

- b. Para determinar qué cucharones tienen las operaciones de SPUT más lentas, utilice `-gb` opción, que agrupa mensajes por bloque:

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

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.cho-non-versioning 1.571	71943	0.046	1770.563
SPUT.cho-versioning 1.415	54277	0.047	1736.633
SPUT.cho-west-region 1.329	80615	0.040	55.557
SPUT.ldt002 0.361	1564563	0.011	51.569

- c. Para determinar qué cucharones tienen el tamaño de objeto SPUT más grande, utilice ambos `-gb` y la `-s` opciones:

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

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

Formato de mensaje de auditoría

Formato del mensaje de auditoría: Información general

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 está reportando.

Si la información resumida proporcionada por el ["auditoría-explicar"](#) y.. ["suma de auditoría"](#) las herramientas son insuficientes; consulte esta sección para comprender el formato general de todos los mensajes de auditoría.

El siguiente es un mensaje de auditoría de ejemplo que puede 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 (FC32) :SYSU] [ANID (UI32) :11627225] [AMID (FC32) :ARNI] [ATID (UI64) :9445736326500603516]]
```

Cada mensaje de auditoría contiene una cadena de elementos de atributo. Toda la cadena se encuentra entre paréntesis ([]), y cada elemento de atributo de la cadena tiene las siguientes características:

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

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

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

El número de elementos de atributo del mensaje depende del tipo de evento del mensaje. Los elementos de atributo no aparecen en ningún orden en particular.

En la siguiente lista se describen los elementos del 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 a otros que son específicos de eventos.
- `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 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 mensajes de auditoría.

Tipo	Descripción
UI32	Entero largo sin signo (32 bits); puede almacenar los números de 0 a 4,294,967,295.
UI64	Entero doble largo sin signo (64 bits); puede almacenar los números de 0 a 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 usa para direcciones IP.
CSTR	Matriz de longitud variable de caracteres UTF-8. Los caracteres se pueden escapar con las siguientes convenciones: <ul style="list-style-type: none">• La barra invertida es \.• El retorno del carro es \r.• Las comillas dobles son \".• La alimentación de línea (nueva línea) es \n.• Los caracteres se pueden sustituir por sus equivalentes hexadecimales (en el formato \xHH, donde HH es el valor hexadecimal que representa el carácter).

Datos específicos de un evento

Cada mensaje de auditoría del registro de auditoría registra datos específicos de un

Codificación	Tipo	Descripción
ATIM	UI64	<p>Marca de hora: Hora en la que se generó el evento que activó el mensaje de auditoría, medida en microsegundos desde la época del sistema operativo (00:00:00 UTC el 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 local se basan en milisegundos.</p> <p>Es posible que sea necesario redondear o truncar la Marca de tiempo registrada. El tiempo legible por el usuario que aparece al principio del mensaje de auditoría en <code>audit.log</code> File es el atributo ATIM en formato ISO 8601. La fecha y la hora se representan como <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code>, donde <code>T</code> es un carácter literal de cadena que indica el comienzo del segmento de tiempo de la fecha. <code>UUUUUU</code> son microsegundos.</p>
ATYP	FC32	Tipo de evento: Identificador de cuatro caracteres del evento que se está registrando. Esto rige el contenido de "carga útil" del mensaje: Los atributos que se incluyen.
PROTECTOR	UI32	Versión: 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 auditorías. Este campo permite la compatibilidad con versiones anteriores del servicio AMS para procesar mensajes de versiones anteriores de servicios.
TRANSFORMACIÓN DIGITAL	FC32	Resultado: Resultado del evento, proceso o transacción. Si no es relevante para un mensaje, NO SE utiliza NINGUNO 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 tienen el mismo formato.

A continuación se muestra un mensaje de auditoría de ejemplo, que puede aparecer en la `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) : "s3small11"] [S3K
Y (CSTR) : "hello1"] [CBID (UI64) : 0x50C4F7AC2BC8EDF7] [CSIZ (UI64) : 0
] [AVER (UI32) : 10] [ATIM (UI64) : 1405631878959669] [ATYP (FC32) : SPUT
] [ANID (UI32) : 12872812] [AMID (FC32) : S3RQ] [ATID (UI64) : 1579224144
102530435]]
```

El mensaje de auditoría contiene información sobre el evento que se está grabando, así como información

sobre el propio mensaje de auditoría.

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

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

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

El siguiente mensaje de auditoría también muestra el bloque 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\):"s3small11"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Para detectar cuándo se produjo el evento PUT, anote la Marca de hora de hora universal coordinada (UTC) al comienzo del mensaje de auditoría. Este valor es una versión legible por 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):"s3small11"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\ (UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

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

Auditar los mensajes y el ciclo de vida del objeto

¿Cuándo se generan los mensajes de auditoría?

Se generan mensajes de auditoría cada vez que se procesa, recupera o elimina un objeto. Puede identificar estas transacciones en el registro de auditoría localizando mensajes de auditoría específicos de la API (S3 o Swift).

Los mensajes de auditoría se vinculan a través de identificadores específicos de cada protocolo.

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

Plazos de los mensajes de auditoría

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

Nodos de archivado

La serie de mensajes de auditoría generados cuando un nodo de archivado envía datos de objeto a un sistema de almacenamiento de archivado externo es similar a la de los nodos de almacenamiento, excepto que no hay ningún mensaje SCMT (confirmación de objeto de almacén), Y los mensajes ATCE (Archive Object Store Begin) y ASCE (Archive Object Store End) se generan para cada copia archivada de datos de objeto.

La serie de mensajes de auditoría generados cuando un nodo de archivado recupera datos de objeto de un sistema de almacenamiento de archivado externo es similar a la de los nodos de almacenamiento, excepto que los mensajes ARCB (Archive Object Retrieve Begin) y ARCE (Archive Object Retrieve End) se generan para cada copia recuperada de los datos de objeto.

La serie de mensajes de auditoría generados cuando un nodo de archivado elimina los datos de objeto de un sistema de almacenamiento de archivado externo es similar a la de los nodos de almacenamiento, excepto que no hay ningún mensaje SREM (Object Store Remove) y hay un mensaje AREM (Archive Object Remove) para cada solicitud de eliminación.

Transacciones de procesamiento de objetos

Puede identificar las transacciones de procesamiento del cliente en el registro de auditoría ubicando mensajes de auditoría específicos de la API (S3 o Swift).

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

Mensajes de auditoría de incorporación de S3

Codificación	Nombre	Descripción	Traza	Consulte
SPUT	Transacción PUT de S3	Una transacción de procesamiento PUT DE S3 se ha completado correctamente.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Se cumplen las reglas del objeto	La política de ILM se ha satisfecho para este objeto.	CBID	"ORLM: Se cumplen las reglas de objeto"

Mensajes de auditoría de procesamiento rápido

Codificación	Nombre	Descripción	Traza	Consulte
WPUT	Transacción DE SWIFT PUT	Se ha completado correctamente una transacción de procesamiento DE PUT de Swift.	CBID, WCON, WOBJ	"WPUT: SWIFT PUT"
ORLM	Se cumplen las reglas del objeto	La política de ILM se ha satisfecho para este objeto.	CBID	"ORLM: Se cumplen las reglas de objeto"

Ejemplo: Ingesta de objetos S3

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

En este ejemplo, la política de ILM activa incluye la regla de ILM Make 2 copies.



En el ejemplo siguiente no se enumeran todos los mensajes de auditoría generados durante una transacción. Solo se muestran los relacionados con la transacción de procesamiento de S3 (SPUT).

En este ejemplo se supone que se ha creado previamente un bloque de S3.

SPUT: S3 PUT

El mensaje SPUT se genera para indicar que se ha emitido una transacción PUT de S3 para crear un objeto en un segmento 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(CSTR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:identity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SBAC(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 la política ILM se ha cumplido con 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 de nodo LDR y el ID de volumen de las ubicaciones de 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 código de borrado, el campo LOCS incluye el identificador de perfil de código de borrado y el identificador de grupo de códigos 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):4168559046473725560]]
```

El campo PATH incluye información sobre el bloque de S3 y claves o información sobre el contenedor y el objeto de Swift, según qué API se haya utilizado.

```

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]]

```

Objeto: Eliminar transacciones

Puede identificar transacciones de eliminación de objetos en el registro de auditoría ubicando mensajes de auditoría específicos de la API (S3 y Swift).

En las tablas siguientes no se enumeran todos los mensajes de auditoría generados durante una transacción de eliminación. Sólo se incluyen los mensajes necesarios para realizar el seguimiento de la transacción de eliminación.

S3 elimina mensajes de auditoría

Codificación	Nombre	Descripción	Traza	Consulte
SDEL	Eliminación de S3	Solicitud realizada para eliminar el objeto de un bloque.	CBID, S3KY	"SDEL: ELIMINACIÓN DE S3"

Elimine mensajes de auditoría de Swift

Codificación	Nombre	Descripción	Traza	Consulte
¡WDEL	Eliminación de Swift	Solicitud realizada para eliminar el objeto de un contenedor o del contenedor.	CBID, WOBJ	"WDEL: ELIMINACIÓN de Swift"

Ejemplo: Eliminación de objetos de 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.



En el ejemplo siguiente no se enumeran todos los mensajes de auditoría generados durante una transacción de eliminación. Solo se muestran los relacionados con la transacción de eliminación de S3 (SDEL).

SDEL: Eliminación S3

La eliminación de objetos comienza cuando el cliente envía una solicitud DE ELIMINACIÓN de objeto a un servicio LDR. El mensaje contiene el bloque del cual se elimina el objeto y la clave S3 del objeto, que se utiliza

para identificar el objeto.

```
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):"SGKHya1RU_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]
```

El objeto recupera las transacciones

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

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

Mensajes de auditoría de recuperación de S3

Codificación	Nombre	Descripción	Traza	Consulte
SGET	S3 TIENE	Solicitud realizada para recuperar un objeto de un bloque.	CBID, S3BK, S3KY	"SGET: S3 GET"

Mensajes de auditoría de recuperación rápida

Codificación	Nombre	Descripción	Traza	Consulte
CONSIGA	OBTENGA Swift	Solicitud realizada para recuperar un objeto de un contenedor.	CBID, WCON, WOBJ	"WGET: Swift GET"

Ejemplo: Recuperación de objetos de 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 se muestran en el siguiente ejemplo. Solo se muestran las relacionadas con la transacción de recuperación de S3 (SGET).

SGET: S3 GET

La recuperación de objetos comienza cuando el cliente envía una solicitud GET Object a un servicio LDR. El mensaje contiene el bloque del cual se puede recuperar el objeto y la clave S3 del objeto, que se utiliza para identificar el objeto.

```

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

En el siguiente mensaje de ejemplo, el cliente envía una solicitud GET Object 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 bloque, que difieren del ID de cuenta de inquilino y del nombre del cliente registrado 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):"SGKHpoblW1P_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):SGE
T][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]

```

Ejemplo: S3 Select en un objeto

Cuando un cliente S3 emite una consulta S3 Select en 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 se muestran en el siguiente ejemplo. Solo se muestran los relacionados con la transacción Select de S3 (SelectObjectContent).

Cada consulta da como resultado dos mensajes de auditoría: Uno que realiza la autorización de la solicitud S3 Select (el campo S3SR está definido en "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:identit
y::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

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

Mensajes de auditoría de actualización de metadatos S3

Codificación	Nombre	Descripción	Traza	Consulte
SUPD	Metadatos de S3 actualizados	Se genera cuando un cliente S3 actualiza los metadatos de un objeto ingerido.	CBID, S3KY, HTRH	"SUPD: Se han actualizado metadatos S3"

Ejemplo: Actualización de metadatos de S3

El ejemplo muestra una transacción correcta 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 las solicitudes se incluyen en el campo HTRH porque se ha configurado como encabezado de protocolo de auditoría (**CONFIGURACIÓN > Supervisión > servidor de auditoría y syslog**). Consulte ["Configurar los mensajes de auditoría y los 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+aVvV01TSYhEGts=\",
\"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]]
```

Auditar mensajes

Mensajes de auditoría: Información general

En las secciones siguientes 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 por la clase de actividad que representa el mensaje. Estas agrupaciones son útiles tanto para comprender los tipos de actividades auditadas como para seleccionar el tipo deseado de filtrado de mensajes de auditoría.

Los mensajes de auditoría también se enumeran alfabéticamente por sus códigos de cuatro caracteres. Esta lista alfabética le permite buscar información sobre mensajes específicos.

Los códigos de cuatro caracteres utilizados en este capítulo son los valores del ATYP encontrados 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 la configuración de niveles de mensajes de auditoría, el cambio de destinos de registro y el uso de un servidor syslog externo para la información de auditoría, consulte ["Configurar los mensajes de auditoría y los destinos de registro"](#)

Auditar categorías de mensajes

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 propio sistema de auditoría, los estados de los nodos de la cuadrícula, la actividad de tareas en todo el sistema (tareas de grid) y las operaciones de copia de seguridad de servicio.

Codificación	Título del mensaje y descripción	Consulte
ECMC	Falta el fragmento de datos con código de borrado: Indica que se ha detectado un fragmento de datos con código de borrado que falta.	"ECMC: Falta el fragmento de datos codificados de borrado"
ECOC	Fragmento de datos con código de borrado dañado: Indica que se ha detectado un fragmento de datos con código de borrado dañado.	"ECOC: Fragmento de datos codificados con borrado dañado"
ETAF	Error en la autenticación de seguridad: Error en un intento de conexión mediante la seguridad de la capa de transporte (TLS).	"ETAF: Error de autenticación de seguridad"
GNRG	Registro de GNDS: Un servicio actualizado o información registrada sobre sí mismo en el sistema StorageGRID.	"GNRG: Registro GNDS"
RNUR	Registro de GNDS: Un servicio se ha registrado de forma no registrada del sistema StorageGRID.	"GNUR: Registro de GNDS"
GTED	Tarea de cuadrícula finalizada: El servicio CMN ha terminado de procesar la tarea de cuadrícula.	"GTED: La tarea de la red terminó"
GTST	Tarea de cuadrícula iniciada: El servicio CMN comenzó a procesar la tarea de cuadrícula.	"GTST: Se ha iniciado la tarea de cuadrícula"
GTSU	Tarea de cuadrícula enviada: Se ha enviado una tarea de cuadrícula al servicio CMN.	"GTSU: Se ha enviado la tarea de la cuadrícula"

Codificación	Título del mensaje y descripción	Consulte
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"
AGREGAR	Deshabilitación de auditoría de seguridad: Se ha desactivado el registro de mensajes de auditoría.	"SADD: Desactivación de auditoría de seguridad"
SADE	Habilitación de auditoría de seguridad: Se ha restaurado el registro de mensajes de auditoría.	"SADE: Activación de auditoría de seguridad"
SRF	Error de verificación del almacén de objetos: Un bloque de contenido ha fallado las comprobaciones de verificación.	"SVRF: Fallo de verificación del almacén de objetos"
SVRU	Verificación de almacén de objetos desconocida: Se han detectado datos de objeto inesperados en el almacén de objetos.	"SVRU: Verificación del almacén de objetos desconocida"
SYSD	Node Stop: Se ha solicitado un apagado.	"SYSD: Parada del nodo"
SYST	Nodo de detención: Un servicio ha iniciado una detención elegante.	"SYST: Nodo detenido"
SYSU	Node Start: Se ha iniciado un servicio; la naturaleza del apagado anterior se indica en el mensaje.	"SYSU: Inicio del nodo"

Mensajes de auditoría del almacenamiento de objetos

Los mensajes de auditoría que pertenecen a la categoría de auditoría del almacenamiento de objetos se utilizan para eventos relacionados con el almacenamiento y la gestión de los objetos dentro del sistema StorageGRID. Entre estas se incluyen las recuperaciones y almacenamiento de objetos, el nodo de grid a transferencias de Grid-nodo y las verificaciones.

Codificación	Descripción	Consulte
APCT	Análisis de archivo desde Cloud-Tier: Los datos de objetos archivados se eliminan de un sistema de almacenamiento de archivado externo, que se conecta a StorageGRID a través de la API S3.	"APCT: Purga de archivos desde la capa de cloud"

Codificación	Descripción	Consulta
ARCB	Inicio de recuperación de objetos de archivo: El servicio ARC inicia la recuperación de datos de objetos desde el sistema de almacenamiento de archivos externo.	"ARCB: Inicio de recuperación de objetos de archivo"
ARCE	Fin de recuperación de objeto de archivo: Los datos de objeto se han recuperado de un sistema de almacenamiento de archivos externo y el servicio ARC informa del estado de la operación de recuperación.	"ARCE: Fin de recuperación de objetos archivados"
ARCT	Recuperación de archivo desde Cloud-Tier: Los datos de objetos archivados se recuperan de un sistema de almacenamiento de archivado externo, que se conecta a StorageGRID a través de la API S3.	"ARCT: Recuperación de archivos a partir de nivel de cloud"
AREM	Eliminación de objetos de archivo: Un bloque de contenido se ha eliminado correctamente o sin éxito del sistema de almacenamiento de archivos externo.	"AREM: Eliminación de objeto de archivado"
ASCE	Fin del almacén de objetos archivados: Se ha escrito un bloque de contenido en el sistema de almacenamiento de archivos externo y el servicio ARC informa del estado de la operación de escritura.	"ASCE: Fin del almacén de objetos de archivo"
ASCT	Almacenamiento de archivos Cloud-Tier: Los datos de objetos se almacenan en un sistema de almacenamiento de archivado externo, que se conecta a la StorageGRID a través de la API de S3.	"ASCT: Archive Store Cloud-Tier"
ATCE	Inicio del almacén de objetos de archivado: Se ha iniciado la escritura de un bloque de contenido en un almacenamiento de archivado externo.	"ATCE: Inicio del almacén de objetos de archivado"
AVCC	Validación de archivo Configuración de nivel de cloud: La configuración de la cuenta y el bloque proporcionados se validó correctamente o sin éxito.	"AVCC: Validación de archivo de la configuración de Cloud-Tier"
BROR	Solicitud de solo lectura de bloque: Un bloque entró o salió del modo de solo lectura.	"BROR: Solicitud de solo lectura de bucket"
CBSE	Objeto Send End: La entidad de origen completó una operación de transferencia de datos de un nodo de cuadrícula a un nodo de cuadrícula.	"CBSE: Fin de envío de objeto"

Codificación	Descripción	Consulta
CBRE	Fin de recepción de objetos: La entidad de destino completó una operación de transferencia de datos de Grid-node hacia Grid-node.	"CBRE: Fin de recepción de objeto"
CGRR	Solicitud de replicación entre grid: StorageGRID intentó realizar una operación de replicación entre grid para replicar objetos entre buckets de una conexión de federación de grid.	"CGRR: Solicitud de Replicación de Cuadrícula Cruzada"
EBDL	Empty Bucket Delete: El análisis de ILM eliminó un objeto de un bloque que está eliminando todos los objetos (realizando una operación de bloque vacía).	"EBDL: Eliminación de bloque vacío"
EBKR	Solicitud de depósito vacío: Un usuario ha enviado una solicitud para activar o desactivar el depósito vacío (es decir, para eliminar objetos de depósito o para dejar de suprimir objetos).	"EBKR: Solicitud de depósito vacío"
SCMT	Confirmación del almacén de objetos: Un bloque de contenido se almacenó y verificó completamente, y ahora se puede solicitar.	"SCMT: Solicitud de confirmación del almacén de objetos"
SREM	Almacén de objetos Quitar: Se ha eliminado un bloque de contenido de un nodo de cuadrícula y ya no se puede solicitar directamente.	"SREM: Almacén de objetos Quitar"

El cliente lee los mensajes de auditoría

Los mensajes de auditoría de lectura de cliente se registran cuando una aplicación cliente S3 o Swift hace una solicitud para recuperar un objeto.

Codificación	Descripción	Utilizado por	Consulta
S3SL	S3 Seleccionar solicitud: Registra una finalización después de que una solicitud de S3 Select se ha devuelto al cliente. El mensaje S3SL puede incluir detalles de mensaje de error y código de error. Es posible que la solicitud no se haya realizado correctamente.	Cliente S3	"S3SL: S3 Seleccione la solicitud"
SGET	S3 GET: Registra una transacción realizada correctamente para recuperar un objeto o enumerar los objetos de un bloque. Nota: Si la transacción opera en un subrecurso, el mensaje de auditoría incluirá el campo S3SR.	Cliente S3	"SGET: S3 GET"

Codificación	Descripción	Utilizado por	Consulte
SHEA	S3 HEAD: Registra una transacción realizada correctamente para comprobar la existencia de un objeto o bloque.	Cliente S3	"SHEA: CABEZA S3"
CONSIGA	Swift GET: Registra una transacción realizada correctamente para recuperar un objeto o enumerar los objetos de un contenedor.	Cliente Swift	"WGET: Swift GET"
WHEA	Swift HEAD: Registra una transacción realizada correctamente para comprobar la existencia de un objeto o contenedor.	Cliente Swift	"WHEA: CABEZA de Swift"

El cliente escribe mensajes de auditoría

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

Codificación	Descripción	Utilizado por	Consulte
OVWR	Objeto Overwrite: Registra una transacción para sobrescribir un objeto con otro.	Clientes S3 y Swift	"OVWR: Sobrescritura de objetos"
SDEL	S3 DELETE: Registra una transacción realizada correctamente para eliminar un objeto o bloque. Nota: Si la transacción opera en un subrecurso, el mensaje de auditoría incluirá el campo S3SR.	Cliente S3	"SDEL: ELIMINACIÓN DE S3"
SPO	S3 POST: Registra una transacción realizada correctamente para restaurar un objeto del almacenamiento AWS Glacier en un Pool de almacenamiento en cloud.	Cliente S3	"SPOS: PUBLICACIÓN DE S3"
SPUT	S3 PUT: Registra una transacción realizada correctamente para crear un nuevo objeto o bloque. Nota: Si la transacción opera en un subrecurso, el mensaje de auditoría incluirá el campo S3SR.	Cliente S3	"SPUT: S3 PUT"
SUPD	S3 Metadata Updated: Registra una transacción correcta para actualizar los metadatos de un objeto o bloque existente.	Cliente S3	"SUPD: Se han actualizado metadatos S3"
¡WDEL	Swift DELETE: Registra una transacción realizada correctamente para eliminar un objeto o un contenedor.	Cliente Swift	"WDEL: ELIMINACIÓN de Swift"

Codificación	Descripción	Utilizado por	Consulte
WPUT	Swift PUT: Registra una transacción correcta para crear un nuevo objeto o contenedor.	Cliente Swift	"WPUT: SWIFT PUT"

Mensaje de auditoría de gestión

La categoría Management registra las solicitudes de usuario a la API de gestión.

Codificación	Título del mensaje y descripción	Consulte
MGAU	Mensaje de auditoría de la API de gestión: Un registro de solicitudes de usuario.	"MGAU: Mensaje de auditoría de gestión"

Mensajes de auditoría de operaciones de ILM

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

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

Referencia de mensajes de auditoría

APCT: Purga de archivos desde la capa de cloud

Este mensaje se genera cuando los datos de objetos archivados se eliminan de un sistema de almacenamiento de archivado externo, que se conecta a la StorageGRID a través de la API S3.

Codificación	Campo	Descripción
CBID	ID del bloque de contenido	Identificador único del bloque de contenido eliminado.

Codificación	Campo	Descripción
CSIZ	Tamaño de contenido	El tamaño del objeto en bytes. Siempre devuelve 0.
TRANSFORMACIÓN DIGITAL	Código de resultado	Devuelve correcto (SUCS) o el error notificado por el backend.
SUID	Identificador único de almacenamiento	Identificador único (UUID) del nivel de cloud desde el que se eliminó el objeto.

ARCB: Inicio de recuperación de objetos de archivo

Este mensaje se genera cuando se realiza una solicitud para recuperar datos de objeto archivados y comienza el proceso de recuperación. Las solicitudes de recuperación se procesan de forma inmediata, pero se pueden reordenar para mejorar la eficacia de la recuperación de medios lineales como, por ejemplo, la cinta.

Codificación	Campo	Descripción
CBID	ID del bloque de contenido	Identificador único del bloque de contenido que se va a recuperar del sistema de almacenamiento de archivos externo.
TRANSFORMACIÓN DIGITAL	Resultado	Indica el resultado de iniciar el proceso de recuperación de archivos. El valor definido actualmente es: SUCS: Se recibió la solicitud de contenido y se puso en cola para su recuperación.

Este mensaje de auditoría Marca el tiempo de una recuperación de archivo. Permite hacer coincidir el mensaje con un mensaje ARCE End correspondiente para determinar la duración de la recuperación del archivo y si la operación se ha realizado correctamente.

ARCE: Fin de recuperación de objetos archivados

Este mensaje se genera cuando finaliza un intento del nodo de archivado de recuperar datos de objeto de un sistema de almacenamiento de archivado externo. Si se realiza correctamente, el mensaje indica que los datos del objeto solicitado se han leído completamente desde la ubicación de archivado y se han verificado correctamente. Una vez que se recuperan y verifican los datos del objeto, se envían al servicio que lo solicita.

Codificación	Campo	Descripción
CBID	ID del bloque de contenido	Identificador único del bloque de contenido que se va a recuperar del sistema de almacenamiento de archivos externo.
VLID	Identificador del volumen	El identificador del volumen en el cual se archivaron los datos. Si no se encuentra una ubicación de archivado para el contenido, se devuelve un ID de volumen 0.

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Resultado de la recuperación	El estado de finalización del proceso de recuperación de archivos: <ul style="list-style-type: none"> • SUCS: Exitoso • VRFL: Error (fallo de verificación del objeto) • ARUN: Error (sistema de almacenamiento de archivado externo no disponible) • CANC: Fallo (operación de recuperación cancelada) • ERROR GENERAL (ERROR general)

La coincidencia de este mensaje con el correspondiente mensaje ARCB puede indicar el tiempo que se tarda en realizar la recuperación del archivo. Este mensaje indica si la recuperación se ha realizado correctamente y, en caso de fallo, la causa del fallo al recuperar el bloque de contenido.

ARCT: Recuperación de archivos a partir de nivel de cloud

Este mensaje se genera cuando se recuperan datos de objetos archivados de un sistema de almacenamiento de archivado externo, que se conecta a la StorageGRID a través de la API de S3.

Codificación	Campo	Descripción
CBID	ID del bloque de contenido	Identificador único del bloque de contenido recuperado.
CSIZ	Tamaño de contenido	El tamaño del objeto en bytes. El valor sólo es preciso para las recuperar correctamente.
TRANSFORMACIÓN DIGITAL	Código de resultado	Devuelve correcto (SUCS) o el error notificado por el backend.
SUID	Identificador único de almacenamiento	Identificador único (UUID) del sistema de almacenamiento de archivado externo.
TIEMPO	Tiempo	Tiempo de procesamiento total de la solicitud en microsegundos.

AREM: Eliminación de objeto de archivado

El mensaje de auditoría Eliminar objeto de archivado indica que un bloque de contenido se eliminó correctamente o de forma incorrecta de un nodo de archivado. Si el resultado es correcto, el nodo de archivado ha informado correctamente al sistema de almacenamiento de archivado externo que StorageGRID ha lanzado una ubicación de objeto. Si el objeto se elimina del sistema de almacenamiento de archivos externo depende del tipo de sistema y de su configuración.

Codificación	Campo	Descripción
CBID	ID del bloque de contenido	Identificador único del bloque de contenido que se va a recuperar del sistema de archivos multimedia externo.
VLID	Identificador del volumen	El identificador del volumen en el que se han archivado los datos de objeto.
TRANSFORMACIÓN DIGITAL	Resultado	El estado de finalización del proceso de eliminación de archivos: <ul style="list-style-type: none"> • SUCS: Exitoso • ARUN: Error (sistema de almacenamiento de archivado externo no disponible) • ERROR GENERAL (ERROR general)

ASCE: Fin del almacén de objetos de archivo

Este mensaje indica que ha finalizado la escritura de un bloque de contenido en un sistema de almacenamiento de archivado externo.

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	Identificador del bloque de contenido almacenado en el sistema de almacenamiento de archivos externo.
VLID	Identificador del volumen	El identificador único del volumen de archivado en el que se escriben los datos de objetos.
REN	Verificación habilitada	Indica si se realiza la verificación para bloques de contenido. Los valores definidos actualmente son: <ul style="list-style-type: none"> • VENA: La verificación está activada • VDSA: La verificación está desactivada
MCLS	Clase de Gestión	Cadena que identifica la clase de gestión de TSM a la que se asigna el bloque de contenido si procede.
TRANSFORMACIÓN DIGITAL	Resultado	Indica el resultado del proceso de archivado. Los valores definidos actualmente son: <ul style="list-style-type: none"> • ÉXITO: Correcto (proceso de archivado realizado correctamente) • OFL: Error (el archivado está sin conexión) • VRFL: Error (fallo de verificación del objeto) • ARUN: Error (sistema de almacenamiento de archivado externo no disponible) • ERROR GENERAL (ERROR general)

Este mensaje de auditoría significa que el bloque de contenido especificado se ha escrito en el sistema de almacenamiento de archivado externo. Si la escritura falla, el resultado ofrece información básica de solución de problemas sobre dónde se produjo el error. Puede encontrar información más detallada acerca de los errores de archivado examinando los atributos del nodo de archivado en el sistema StorageGRID.

ASCT: Archive Store Cloud-Tier

Este mensaje se genera cuando los datos de objetos archivados se almacenan en un sistema de almacenamiento de archivado externo, que se conecta a StorageGRID a través de la API S3.

Codificación	Campo	Descripción
CBID	ID del bloque de contenido	Identificador único del bloque de contenido recuperado.
CSIZ	Tamaño de contenido	El tamaño del objeto en bytes.
TRANSFORMACIÓN DIGITAL	Código de resultado	Devuelve correcto (SUCS) o el error notificado por el backend.
SUID	Identificador único de almacenamiento	Identificador único (UUID) del nivel de cloud al que se almacenó el contenido.
TIEMPO	Tiempo	Tiempo de procesamiento total de la solicitud en microsegundos.

ATCE: Inicio del almacén de objetos de archivado

Este mensaje indica que se ha iniciado la escritura de un bloque de contenido en un almacenamiento de archivado externo.

Codificación	Campo	Descripción
CBID	ID del bloque de contenido	Identificador único del bloque de contenido que se va a archivar.
VLID	Identificador del volumen	Identificador único del volumen en el que se escribe el bloque de contenido. Si se produce un error en la operación, se devuelve un ID de volumen 0.

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Resultado	Indica el resultado de la transferencia del bloque de contenido. Los valores definidos actualmente son: <ul style="list-style-type: none"> • ÉXITO (bloque de contenido almacenado correctamente) • EXIS: Ignorado (el bloque de contenido ya estaba almacenado) • ISFD: Error (espacio en disco insuficiente) • STER: Error (error al almacenar el CBID) • OFL: Error (el archivado está sin conexión) • ERROR GENERAL (ERROR general)

AVCC: Validación de archivo de la configuración de Cloud-Tier

Este mensaje se genera cuando se validan las opciones de configuración para un tipo de destino Cloud Tiering: Simple Storage Service (S3).

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Código de resultado	Devuelve correcto (SUCS) o el error notificado por el backend.
SUID	Identificador único de almacenamiento	UUID asociado con la validación del sistema de almacenamiento de archivado externo.

BROR: Solicitud de solo lectura de bucket

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

Codificación	Campo	Descripción
BKHD	UUID de bloque	El ID de bloque.
BROV	Valor de solicitud de sólo lectura del segmento	Si el depósito se está convirtiendo en de solo lectura o si está dejando el estado de solo lectura (1 = de solo lectura, 0 = no de solo lectura).
BROS	Motivo de sólo lectura del depósito	El motivo por el que el depósito se convierte en de sólo lectura o deja el estado de sólo lectura. Por ejemplo, emptyBucket.
S3AI	S3 ID de cuenta de inquilino	El ID de la cuenta de inquilino que envió la solicitud. Un valor vacío indica acceso anónimo.

Codificación	Campo	Descripción
S3BK	S3 cucharón	El nombre de bloque de S3.

CBRB: Inicio de recepción de objetos

Durante las operaciones normales del sistema, los bloques de contenido se transfieren de forma continua 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.

Codificación	Campo	Descripción
CNID	Identificador de conexión	El identificador único de la sesión/conexión nodo a nodo.
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido que se está transfiriendo.
CTDR	Dirección de transferencia	Indica si la transferencia CBID se inició mediante inserción o se inició con extracción: INSERCIÓN: La entidad emisora solicitó la operación de transferencia. PULL: La entidad receptora solicitó la operación de transferencia.
CTSR	Entidad de origen	El ID de nodo de la fuente (remitente) de la transferencia CBID.
CTD	Entidad de destino	El ID de nodo del destino (receptor) de la transferencia CBID.
CTSS	Recuento de secuencias de inicio	Indica el primer recuento de secuencias solicitado. Si la transferencia se realiza correctamente, comienza a partir del número de secuencias.
CTE	Recuento de secuencias finales esperadas	Indica el último recuento de secuencias solicitado. Si se realiza correctamente, la transferencia se considera completa cuando se ha recibido este recuento de secuencias.
TRANSFORMACIÓN DIGITAL	Estado de inicio de transferencia	Estado en el momento en que se inició la transferencia: SUCS: La transferencia se inició correctamente.

Este mensaje de auditoría significa que se ha iniciado una operación de transferencia de datos nodo a nodo en un único elemento de contenido, según lo identifica su identificador de bloque de contenido. La operación solicita datos de "Start Sequence Count" a "Contador de secuencia final esperado". El envío y la recepción de

nodos se identifican mediante sus ID de nodo. Esta información se puede utilizar para realizar un seguimiento del flujo de datos del sistema y, cuando se combina con mensajes de auditoría de almacenamiento, para comprobar el número de réplicas.

CBRE: Fin de recepción de objeto

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

Codificación	Campo	Descripción
CNID	Identificador de conexión	El identificador único de la sesión/conexión nodo a nodo.
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido que se está transfiriendo.
CTDR	Dirección de transferencia	Indica si la transferencia CBID se inició mediante inserción o se inició con extracción: INSERCIÓN: La entidad emisora solicitó la operación de transferencia. PULL: La entidad receptora solicitó la operación de transferencia.
CTSR	Entidad de origen	El ID de nodo de la fuente (remitente) de la transferencia CBID.
CTD	Entidad de destino	El ID de nodo del destino (receptor) de la transferencia CBID.
CTSS	Recuento de secuencias de inicio	Indica el recuento de secuencias en el que se inició la transferencia.
CTA	Recuento de secuencias finales reales	Indica que el último número de secuencias se ha transferido correctamente. Si el recuento de secuencia final real es el mismo que el recuento de secuencia de inicio y el resultado de la transferencia no se realizó correctamente, no se intercambiaron datos.

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Resultado de la transferencia	<p>El resultado de la operación de transferencia (desde el punto de vista de la entidad emisora):</p> <p>SUCS: Transferencia finalizada correctamente; se enviaron todos los conteos de secuencia solicitados.</p> <p>CONL: Conexión perdida durante la transferencia</p> <p>CTMO: Tiempo de espera de la conexión durante el establecimiento o la transferencia</p> <p>UNRE: No se puede acceder al ID del nodo de destino</p> <p>CRPT: La transferencia finalizó debido a la recepción de datos corruptos o no válidos</p>

Este mensaje de auditoría significa que se completó una operación de transferencia de datos nodo a nodo. Si el resultado de la transferencia se realizó correctamente, la operación transfirió datos de "Start Sequence Count" a "Real End Sequence Count". El envío y la recepción de nodos se identifican mediante sus ID de nodo. Esta información se puede utilizar para realizar un seguimiento del flujo de datos del sistema y localizar, tabular y analizar errores. Cuando se combina con mensajes de auditoría de almacenamiento, también se puede utilizar para verificar el número de réplicas.

CBSB: Inicio de envío de objeto

Durante las operaciones normales del sistema, los bloques de contenido se transfieren de forma continua 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.

Codificación	Campo	Descripción
CNID	Identificador de conexión	El identificador único de la sesión/conexión nodo a nodo.
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido que se está transfiriendo.
CTDR	Dirección de transferencia	<p>Indica si la transferencia CBID se inició mediante inserción o se inició con extracción:</p> <p>INSERCIÓN: La entidad emisora solicitó la operación de transferencia.</p> <p>PULL: La entidad receptora solicitó la operación de transferencia.</p>
CTSR	Entidad de origen	El ID de nodo de la fuente (remitente) de la transferencia CBID.

Codificación	Campo	Descripción
CTD	Entidad de destino	El ID de nodo del destino (receptor) de la transferencia CBID.
CTSS	Recuento de secuencias de inicio	Indica el primer recuento de secuencias solicitado. Si la transferencia se realiza correctamente, comienza a partir del número de secuencias.
CTE	Recuento de secuencias finales esperadas	Indica el último recuento de secuencias solicitado. Si se realiza correctamente, la transferencia se considera completa cuando se ha recibido este recuento de secuencias.
TRANSFORMACIÓN DIGITAL	Estado de inicio de transferencia	Estado en el momento en que se inició la transferencia: SUCS: La transferencia se inició correctamente.

Este mensaje de auditoría significa que se ha iniciado una operación de transferencia de datos nodo a nodo en un único elemento de contenido, según lo identifica su identificador de bloque de contenido. La operación solicita datos de "Start Sequence Count" a "Contador de secuencia final esperado". El envío y la recepción de nodos se identifican mediante sus ID de nodo. Esta información se puede utilizar para realizar un seguimiento del flujo de datos del sistema y, cuando se combina con mensajes de auditoría de almacenamiento, para comprobar el número de réplicas.

CBSE: Fin de envío de objeto

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

Codificación	Campo	Descripción
CNID	Identificador de conexión	El identificador único de la sesión/conexión nodo a nodo.
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido que se está transfiriendo.
CTDR	Dirección de transferencia	Indica si la transferencia CBID se inició mediante inserción o se inició con extracción: INSERCIÓN: La entidad emisora solicitó la operación de transferencia. PULL: La entidad receptora solicitó la operación de transferencia.
CTSR	Entidad de origen	El ID de nodo de la fuente (remitente) de la transferencia CBID.

Codificación	Campo	Descripción
CTD	Entidad de destino	El ID de nodo del destino (receptor) de la transferencia CBID.
CTSS	Recuento de secuencias de inicio	Indica el recuento de secuencias en el que se inició la transferencia.
CTA	Recuento de secuencias finales reales	Indica que el último número de secuencias se ha transferido correctamente. Si el recuento de secuencia final real es el mismo que el recuento de secuencia de inicio y el resultado de la transferencia no se realizó correctamente, no se intercambiaron datos.
TRANSFORMACIÓN DIGITAL	Resultado de la transferencia	El resultado de la operación de transferencia (desde el punto de vista de la entidad emisora): SUCS: Transferencia finalizada correctamente; se enviaron todos los conteos de secuencia solicitados. CONL: Conexión perdida durante la transferencia CTMO: Tiempo de espera de la conexión durante el establecimiento o la transferencia UNRE: No se puede acceder al ID del nodo de destino CRPT: La transferencia finalizó debido a la recepción de datos corruptos o no válidos

Este mensaje de auditoría significa que se completó una operación de transferencia de datos nodo a nodo. Si el resultado de la transferencia se realizó correctamente, la operación transfirió datos de "Start Sequence Count" a "Real End Sequence Count". El envío y la recepción de nodos se identifican mediante sus ID de nodo. Esta información se puede utilizar para realizar un seguimiento del flujo de datos del sistema y localizar, tabular y analizar errores. Cuando se combina con mensajes de auditoría de almacenamiento, también se puede utilizar para verificar el número de réplicas.

CGRR: Solicitud de Replicación de Cuadrícula Cruzada

Este mensaje se genera cuando StorageGRID intenta realizar una operación de replicación entre grid para replicar objetos entre buckets de una conexión de federación de grid. Se envía un mensaje de auditoría sólo si la solicitud ha fallado permanentemente (RESULTADO GERR).

Codificación	Campo	Descripción
S3AI	S3 ID de cuenta de inquilino	ID de la cuenta de inquilino propietaria del depósito desde el que se replica el objeto.

Codificación	Campo	Descripción
GFID	ID de conexión de federación de grid	El ID de la conexión de federación de grid que se utiliza para la replicación entre grid.
OPERATIVO	Funcionamiento de CGR	Tipo de operación de replicación entre grid que se intentó: <ul style="list-style-type: none"> • 0 = Replicar objeto • 1 = Replicar objeto multiparte • 2 = Replicar marcador de borrado
S3BK	S3 cucharón	El nombre de bloque de S3.
S3KY	Clave de S3	El nombre de clave S3, sin incluir el nombre del bloque.
VSID	ID de versión	ID de versión de la versión específica de un objeto que se estaba replicando.
TRANSFORMACIÓN DIGITAL	Código de resultado	Devuelve el error correcto (SUCS) o general (GERR).

EBDL: Eliminación de bloque vacío

El análisis de ILM eliminó un objeto de un bloque que elimina todos los objetos (mediante una operación de bloque vacío).

Codificación	Campo	Descripción
CSIZ	Tamaño del objeto	El tamaño del objeto en bytes.
RUTA	S3 Cubo/llave	El nombre del cubo S3 y el nombre de la clave S3.
SEGC	UUID de contenedor	UUID del contenedor para el objeto segmentado. Este valor sólo está disponible si el objeto está segmentado.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
TRANSFORMACIÓN DIGITAL	Resultado de la operación de supresión	El resultado del evento, proceso o transacción. Si no es relevante para un mensaje, NO SE utiliza NINGUNO en lugar de SUCS para que el mensaje no se filtre accidentalmente.

EBKR: Solicitud de depósito vacío

Este mensaje indica que un usuario ha enviado una solicitud para activar o desactivar el

depósito vacío (es decir, para suprimir objetos de depósito o para dejar de suprimir objetos).

Codificación	Campo	Descripción
BUID	UUID de bloque	El ID de bloque.
EBJS	Configuración de JSON de bloque vacío	Contiene el JSON que representa la configuración actual del bucket vacío.
S3AI	S3 ID de cuenta de inquilino	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Bloque de S3	El nombre de bloque de S3.

ECMC: Falta el fragmento de datos codificados de borrado

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

Codificación	Campo	Descripción
VCMC	ID DEL VCS	El nombre del VCS que contiene el fragmento que falta.
ID DEL MCID	ID de fragmento	El identificador del fragmento con código de borrado que falta.
TRANSFORMACIÓN DIGITAL	Resultado	Este campo tiene el valor 'NONE'. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje en particular. 'NINGUNO' se utiliza en lugar de 'UCS' para que este mensaje no se filtre.

ECOC: Fragmento de datos codificados con borrado dañado

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

Codificación	Campo	Descripción
VCCO	ID DEL VCS	El nombre del VCS que contiene el fragmento dañado.
VLID	ID del volumen	El volumen RangeDB que contiene el fragmento con código de borrado dañado.
CCID	ID de fragmento	El identificador del fragmento codificado por borrado dañado.

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Resultado	Este campo tiene el valor 'NONE'. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje en particular. 'NINGUNO' se utiliza en lugar de 'UCS' para que este mensaje no se filtre.

ETAF: Error de autenticación de seguridad

Este mensaje se genera cuando se produce un error en un intento de conexión mediante la seguridad de la capa de transporte (TLS).

Codificación	Campo	Descripción
CNID	Identificador de conexión	Identificador único del sistema para la conexión TCP/IP a través de la cual falló la autenticación.
RUID	Identidad del usuario	Identificador dependiente del servicio que representa la identidad del usuario remoto.
TRANSFORMACIÓN DIGITAL	Código de razón	El motivo del fallo: SCNI: Error en el establecimiento de conexión segura. CERM: Falta el certificado. CERTIFICADO: El certificado no es válido. CERE: El certificado ha caducado. CERR: Se revocó el certificado. CSGN: La firma del certificado no era válida. CSGU: El firmante del certificado era desconocido. UCRM: Faltan credenciales de usuario. UCRI: Las credenciales de usuario no son válidas. UCRU: No se han permitido las credenciales de usuario. TOUT: Tiempo de espera de autenticación agotado.

Cuando se establece una conexión a un servicio seguro que utiliza TLS, las credenciales de la entidad remota se verifican mediante el perfil TLS y la lógica adicional integrada en el servicio. Si la autenticación no funciona debido a certificados o credenciales no válidos, inesperados o permitidos, se registra un mensaje de auditoría. De esta forma, se pueden realizar consultas para intentos de acceso no autorizados y otros problemas de conexión relacionados con la seguridad.

El mensaje puede resultar de que una entidad remota tenga una configuración incorrecta o de intentos de presentar credenciales no válidas o no permitidas al sistema. Este mensaje de auditoría se debe supervisar

para detectar intentos de 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.

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Resultado	Resultado de la solicitud de actualización: <ul style="list-style-type: none">• SUCS: Exitoso• SVNU: Servicio no disponible• GERR: Otro fracaso
GNID	ID de nodo	El ID de nodo del servicio que inició la solicitud de actualización.
Gntp	Tipo de dispositivo	Tipo de dispositivo del nodo de cuadrícula (por ejemplo, BLDR para un servicio LDR).
GNDV	Versión de modelo de dispositivo	La cadena que identifica la versión del modelo de dispositivo del nodo de cuadrícula en el paquete DMDL.
GNGP	Grupo	El grupo al que pertenece el nodo de cuadrícula (en el contexto de los costes de enlace y la clasificación de consulta de servicio).
GNIA	Dirección IP	La dirección IP del nodo de grid.

Este mensaje se genera siempre que un nodo de grid actualiza su entrada en el paquete Grid Nodes.

GNUR: Registro de GNDS

El servicio CMN genera este mensaje de auditoría cuando un servicio tiene información sin registrar sobre sí mismo desde el sistema StorageGRID.

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Resultado	Resultado de la solicitud de actualización: <ul style="list-style-type: none">• SUCS: Exitoso• SVNU: Servicio no disponible• GERR: Otro fracaso
GNID	ID de nodo	El ID de nodo del servicio que inició la solicitud de actualización.

GTED: La tarea de la red terminó

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 iniciado tarea de cuadrícula correspondiente. Los otros resultados indican que el procesamiento de esta tarea de cuadrícula nunca se ha iniciado.

Codificación	Campo	Descripción
TSID	ID de la tarea	<p>Este campo identifica de forma única una tarea de cuadrícula generada y permite gestionar la tarea de cuadrícula a lo largo de su ciclo de vida.</p> <p>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 enviados, iniciados y terminados.</p>
TRANSFORMACIÓN DIGITAL	Resultado	<p>El resultado final del estado de la tarea de la cuadrícula:</p> <ul style="list-style-type: none">• SUCS: La tarea de la red se completó correctamente.• ABRT: La tarea de cuadrícula ha finalizado sin un error de rollback.• ROLF: La tarea de cuadrícula ha finalizado y no ha podido completar el proceso de rollback.• CANC: La tarea de cuadrícula fue cancelada por el usuario antes de iniciarse.• EXPR: La tarea de la cuadrícula ha caducado antes de iniciarse.• IVLD: La tarea de la cuadrícula no era válida.• AUTH: La tarea de la cuadrícula no estaba autorizada.• DUPL: La tarea de la cuadrícula se rechazó como duplicado.

GTST: Se ha iniciado la tarea de cuadrícula

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

Codificación	Campo	Descripción
TSID	ID de la tarea	Este campo identifica de forma única una tarea de cuadrícula generada y permite gestionar la tarea 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 enviados, iniciados y terminados.
TRANSFORMACIÓN DIGITAL	Resultado	El resultado. Este campo solo tiene un valor: • SUCS: La tarea de red se inició correctamente.

GTSU: Se ha enviado la tarea de la cuadrícula

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

Codificación	Campo	Descripción
TSID	ID de la tarea	Identifica de forma única una tarea de cuadrícula generada y permite gestionar la tarea 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 enviados, iniciados y terminados.
TTYP	Tipo de tarea	Tipo de tarea de cuadrícula.
TVER	Versión de la tarea	Número que indica la versión de la tarea de cuadrícula.
TDSC	Descripción de la tarea	Una descripción legible por el usuario de la tarea de cuadrícula.
VATS	Válido después de la Marca de hora	El primer momento (UINT64 microsegundos a partir del 1 de enero de 1970 - tiempo UNIX) en el que es válida la tarea de la cuadrícula.
VBTS	Válido antes de la Marca de hora	La última hora (UINT64 microsegundos a partir del 1 de enero de 1970 - tiempo UNIX) en la que es válida la tarea de la cuadrícula.

Codificación	Campo	Descripción
TSRC	Origen	El origen de la tarea: <ul style="list-style-type: none"> • TXTB: La tarea de la cuadrícula se envió a través del sistema StorageGRID como un bloque de texto firmado. • CUADRÍCULA: La tarea de la cuadrícula se envió a través del servicio interno de envío de tareas de la cuadrícula.
ACTV	Tipo de activación	Tipo de activación: <ul style="list-style-type: none"> • AUTO: La tarea de cuadrícula se envió para la activación automática. • PEND: La tarea de cuadrícula se ha enviado a la tabla pendiente. Esta es la única posibilidad para la fuente TXTB.
TRANSFORMACIÓN DIGITAL	Resultado	El resultado de la presentación: <ul style="list-style-type: none"> • SUCS: La tarea de la red se envió correctamente. • ERROR: La tarea se ha movido directamente a la tabla histórica.

IDEL: Eliminación de ILM iniciada

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 compatibles con bloques S3:** Este mensaje se genera cuando ILM inicia el proceso de eliminación automática de un objeto debido a que su período de retención ha caducado (suponiendo que la configuración de eliminación automática está activada y la retención legal está desactivada).
- **Para objetos en cubos S3 o contenedores Swift** que no cumplen las normativas. Este mensaje se genera cuando ILM inicia el proceso de eliminación de un objeto porque no hay instrucciones de ubicación en la política de ILM activa actualmente se aplican al objeto.

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	El CBID del objeto.
CMPA	Cumplimiento: Eliminación automática	Para objetos solo en bloques de S3 que cumplen con la normativa. 0 (falso) o 1 (verdadero), que indica si un objeto compatible debe eliminarse automáticamente cuando finalice su período de retención, a menos que el segmento se encuentre bajo una retención legal.
CMPL	Cumplimiento: Conservación legal	Para objetos solo en bloques de S3 que cumplen con la normativa. 0 (falso) o 1 (verdadero), que indica si el cubo está actualmente bajo un derecho.

Codificación	Campo	Descripción
CMPR	Cumplimiento: Período de retención	Para objetos solo en bloques de S3 que cumplen con la normativa. La duración del período de retención del objeto en minutos.
CTME	Cumplimiento de normativas: Tiempo de consumo	Para objetos solo en bloques de S3 que cumplen con la normativa. Tiempo de procesamiento del objeto. Puede agregar el período de retención en minutos a este valor para determinar cuándo se puede eliminar el objeto del bloque.
DMRK	Eliminar ID de versión del marcador	El código de versión del marcador de borrado creado al eliminar un objeto de un bloque con versiones. Las operaciones en los depósitos no incluyen este campo.
CSIZ	Tamaño de contenido	El tamaño del objeto en bytes.
BLOQUEOS	Ubicaciones	<p>La ubicación de almacenamiento de los datos del objeto dentro del sistema StorageGRID. El valor para LOCS es "" si el objeto no tiene ubicaciones (por ejemplo, se ha eliminado).</p> <p>CLEC: En lo que respecta a los objetos codificados de borrado, el ID de perfil de codificación de borrado y el ID de grupo de codificación de borrado que se aplican a los datos del objeto.</p> <p>CLDI: Para los objetos replicados, el ID de nodo LDR y el ID de volumen de la ubicación del objeto.</p> <p>CLNL: ID de nodo DE ARCO de la ubicación del objeto si se archivan los datos del objeto.</p>
RUTA	S3 Bucket/Key o Swift Container/Object ID	El nombre de bloque de S3 y el nombre de clave S3, o el nombre del contenedor de Swift y el identificador de objetos de Swift.
TRANSFORMACIÓN DIGITAL	Resultado	<p>Resultado de la operación de ILM.</p> <p>SUCS: La operación de ILM fue exitosa.</p>
REGLA	Etiqueta de reglas	<ul style="list-style-type: none"> • Si un objeto de un bloque de S3 compatible se elimina automáticamente debido a que su período de retención ha caducado, este campo está en blanco. • Si el objeto se está eliminando porque no hay más instrucciones de ubicación que se apliquen actualmente al objeto, este campo muestra la etiqueta legible para seres humanos de la última regla de ILM que se aplicó al objeto.

Codificación	Campo	Descripción
SGRP	Planta (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 código de versión de la versión específica de un objeto que se eliminó. Las operaciones en cubos y objetos en depósitos sin versiones no incluyen este campo.

LKCU: Limpieza de objetos sobrescritos

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

Codificación	Campo	Descripción
CSIZ	Tamaño de contenido	El tamaño del objeto en bytes.
LLEYP	Tipo de limpieza	<i>Uso interno solamente.</i>
LUID	UUID de objeto eliminado	Identificador del objeto que se ha eliminado.
RUTA	S3 Bucket/Key o Swift Container/Object ID	El nombre de bloque de S3 y el nombre de clave S3, o el nombre del contenedor de Swift y el identificador de objetos de Swift.
SEGC	UUID de contenedor	UUID del contenedor para el objeto segmentado. Este valor sólo está disponible si el objeto está segmentado.
UUID	Identificador único universal	Identificador del objeto que sigue existiendo. Este valor sólo está disponible si el objeto no se ha eliminado.

LLST: Ubicación perdida

Este mensaje se genera siempre que no se encuentra una ubicación para una copia de objeto (replicada o con código de borrado).

Codificación	Campo	Descripción
CBIL	CBID	El CBID afectado.
EPR	Perfil de código de borrado	Para datos de objetos codificados mediante borrado. El código del perfil de código de borrado utilizado.
LLEYP	Tipo de ubicación	CLDI (Online): Para datos de objeto replicados CLEC (en línea): Para datos de objetos codificados con borrado CLNL (Nearline): Para los datos de objetos replicados archivados
NOID	ID del nodo de origen	El ID de nodo en el que se han perdido las ubicaciones.
PCLD	Ruta al objeto replicado	La ruta completa a la ubicación del disco de los datos de objeto perdidos. Sólo se devuelve cuando LTYP tiene un valor de CLDI (es decir, para objetos replicados). Toma la forma <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U}SeUFxE@</code>
TRANSFORMACIÓN DIGITAL	Resultado	Siempre ninguno. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. NO SE utiliza NINGUNO en lugar de SUCS para que este mensaje no se filtre.
TSRC	Origen de activación	USUARIO: Activado por el usuario SYST: Sistema activado
UUID	ID único universal	El identificador del objeto afectado del sistema StorageGRID.

MGAU: Mensaje de auditoría de gestión

La categoría Management registra las solicitudes de usuario a la API de gestión. Cada solicitud que no sea UNA solicitud GET o HEAD a la API registra una respuesta con el nombre de usuario, la IP y el tipo de solicitud a la API.

Codificación	Campo	Descripción
MDIP	Dirección IP de destino	La dirección IP del servidor (destino).
ADN MADN	Nombre de dominio	El nombre de dominio del host.

Codificación	Campo	Descripción
MPAT	RUTA de la solicitud	La ruta de la solicitud.
MPQP	Solicitar parámetros de consulta	Los parámetros de consulta para la solicitud.
MRBD	Solicitar el cuerpo	<p>El contenido del cuerpo de la solicitud. Mientras el cuerpo de respuesta está registrado de forma predeterminada, el cuerpo de la solicitud se registra en determinados casos cuando el cuerpo de respuesta está vacío. Debido a que la siguiente información no está disponible en el cuerpo de respuesta, se toma del organismo de solicitud para los siguientes métodos POST:</p> <ul style="list-style-type: none"> • Nombre de usuario e ID de cuenta en AUTORIZACIÓN DE ENVÍO • Nueva configuración de subredes en POST /grid/grid-Networks/update • Nuevos servidores NTP en POST /grid/ntp-Server/update • ID de servidor retirado en POST /grid/servidores/decomisionate <p>Nota: la información confidencial se elimina (por ejemplo, una clave de acceso S3) o se oculta con asteriscos (por ejemplo, una contraseña).</p>
MRMD	Método de solicitud	<p>El método de solicitud HTTP:</p> <ul style="list-style-type: none"> • PUBLICAR • PUESTO • ELIMINAR • PARCHE
MRSC	Código de respuesta	El código de respuesta.
MRSP	Cuerpo de respuesta	<p>El contenido de la respuesta (el cuerpo de la respuesta) se registra de forma predeterminada.</p> <p>Nota: la información confidencial se elimina (por ejemplo, una clave de acceso S3) o se oculta con asteriscos (por ejemplo, una contraseña).</p>
MSIP	Dirección IP de origen	La dirección IP del cliente (origen).
MUUN	URN de usuario	El URN (nombre de recurso uniforme) del usuario que envió la solicitud.
TRANSFORMACIÓN DIGITAL	Resultado	Devuelve correcto (SUCS) o el error notificado 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.

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	El CBID del objeto perdido.
NOID	ID de nodo	Si está disponible, la última ubicación directa o casi en línea conocida del objeto perdido. Es posible tener solo el ID de nodo sin un ID de volumen si la información del volumen no está disponible.
RUTA	S3 Bucket/Key o Swift Container/Object ID	Si está disponible, el nombre del bloque de S3 y el nombre de la clave S3, o el nombre del contenedor de Swift y el identificador de objetos de Swift.
TRANSFORMACIÓN DIGITAL	Resultado	Este campo no tiene el valor NONE. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. NO SE utiliza NINGUNO en lugar de SUCS para que este mensaje no se filtre.
UUID	ID único universal	El identificador del objeto perdido dentro del sistema StorageGRID.
VOLI	ID del volumen	Si está disponible, el ID de volumen del nodo de almacenamiento o del nodo de archivado de la última ubicación conocida del objeto perdido.

ORLM: Se cumplen las reglas de objeto

Este mensaje se genera cuando el objeto se almacena correctamente y se copia como se especifica en las reglas de ILM.



El mensaje ORLM no se genera cuando un objeto se almacena correctamente mediante la regla de creación de 2 copias predeterminada si otra regla de la directiva utiliza el filtro avanzado Tamaño de objeto.

Codificación	Campo	Descripción
BUID	Cabezal del cucharón	Campo ID de bloque. Se usa para operaciones internas. Sólo aparece si STAT es PRGD.
CBID	Identificador de bloque de contenido	El CBID del objeto.

Codificación	Campo	Descripción
CSIZ	Tamaño de contenido	El tamaño del objeto en bytes.
BLOQUEOS	Ubicaciones	<p>La ubicación de almacenamiento de los datos del objeto dentro del sistema StorageGRID. El valor para LOCS es "" si el objeto no tiene ubicaciones (por ejemplo, se ha eliminado).</p> <p>CLEC: En lo que respecta a los objetos codificados de borrado, el ID de perfil de codificación de borrado y el ID de grupo de codificación de borrado que se aplican a los datos del objeto.</p> <p>CLDI: Para los objetos replicados, el ID de nodo LDR y el ID de volumen de la ubicación del objeto.</p> <p>CLNL: ID de nodo DE ARCO de la ubicación del objeto si se archivan los datos del objeto.</p>
RUTA	S3 Bucket/Key o Swift Container/Object ID	El nombre de bloque de S3 y el nombre de clave S3, o el nombre del contenedor de Swift y el identificador de objetos de Swift.
TRANSFORMACIÓN DIGITAL	Resultado	<p>Resultado de la operación de ILM.</p> <p>SUCS: La operación de ILM fue exitosa.</p>
REGLA	Etiqueta de reglas	La etiqueta legible para seres humanos proporcionada a la regla ILM aplicada a este objeto.
SEGC	UUID de contenedor	UUID del contenedor para el objeto segmentado. Este valor sólo está disponible si el objeto está segmentado.
SGCB	CBID del contenedor	CBID del contenedor del objeto segmentado. Este valor sólo está disponible para objetos segmentados y multipartes.
URGENTE	Estado	<p>El estado de la operación de ILM.</p> <p>DONE: Se completaron las operaciones de ILM contra el objeto.</p> <p>DFER: El objeto se ha marcado para una futura reevaluación de ILM.</p> <p>PRGD: El objeto se ha eliminado del sistema StorageGRID.</p> <p>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.</p>
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.

Codificación	Campo	Descripción
VSID	ID de versión	El código de versión de un nuevo objeto creado en un bloque con versiones. Las operaciones en cubos y objetos en depósitos sin versiones no incluyen este campo.

El mensaje de auditoría ORLM se puede emitir más de una vez para un solo objeto. Por ejemplo, se emite cada vez que ocurre uno de los siguientes eventos:

- Las reglas de ILM para el objeto se satisfacen para siempre.
- Las reglas de ILM para el objeto se satisfacen para esta época.
- Las reglas de ILM se eliminaron el objeto.
- El proceso de verificación en segundo plano detecta que una copia de los datos del objeto replicados está dañada. El sistema StorageGRID realiza una evaluación de ILM para reemplazar el objeto dañado.

Información relacionada

- ["Transacciones de procesamiento de objetos"](#)
- ["Objeto: Eliminar transacciones"](#)

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.

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido (nuevo)	CBID para el nuevo objeto.
CSIZ	Tamaño de objeto anterior	El tamaño, en bytes, del objeto que se sobrescribe.
OCBD	Identificador de bloque de contenido (anterior)	El CBID del objeto anterior.
UUID	ID único universal (nuevo)	El identificador del nuevo objeto dentro del sistema StorageGRID.
OUID	ID único universal (anterior)	El identificador del objeto anterior dentro del sistema StorageGRID.

Codificación	Campo	Descripción
RUTA	La ruta de objetos S3 o Swift	La ruta de objetos S3 o Swift utilizada para el objeto nuevo y el anterior
TRANSFORMACIÓN DIGITAL	Código de resultado	Resultado de la transacción de sobrescritura de objetos. El resultado es siempre: SUCS: Exitoso
SGRP	Planta (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: S3 Seleccione la solicitud

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

Codificación	Campo	Descripción
BYSC	Bytes explorados	Número de bytes explorados (recibidos) de los nodos de almacenamiento. Es probable que BYSC y BYPR sean diferentes si el objeto está comprimido. Si el objeto está comprimido, BYSC tendría el recuento de bytes comprimidos y BYPR sería el bytes después de la descompresión.
BYPR	Bytes procesados	Número de bytes procesados. Indica cuántos bytes de bytes escaneados se procesaron o actuaron realmente en un trabajo de S3 Select.
BYRT	Bytes devueltos	Número de bytes que un trabajo de S3 Select devolvió al cliente.
REPR	Registros procesados	Número de registros o filas que un trabajo de S3 Select ha recibido de los nodos de almacenamiento.
RERT	Registros devueltos	Núm. De registros o filas devueltas al cliente por un trabajo de S3 Select.
JOFI	Trabajo terminado	Indica si el trabajo de S3 Select ha terminado de procesarse o no. Si esto es falso, el trabajo no se ha completado y los campos de error probablemente tendrán datos en ellos. Es posible que el cliente haya recibido resultados parciales o que no haya resultado alguno.
REID	ID de solicitud	Identificador para la solicitud S3 Select.

Codificación	Campo	Descripción
EXTM	Tiempo de ejecución	El tiempo, en segundos, que tardó en completarse el trabajo de selección de S3.
ERMG	Mensaje de error	Mensaje de error que ha generado el trabajo S3 Select.
ERTY	Tipo de error	Tipo de error generado por el trabajo S3 Select.
ERST	Error Stacktrace	Error Stacktrace generado por el trabajo S3 Select.
S3BK	S3 cucharón	El nombre de bloque de S3.
S3AK	ID de clave de acceso S3 (remitente de solicitudes)	El ID de clave de acceso S3 para el usuario que envió la solicitud.
S3AI	ID de cuenta de inquilino de S3 (remitente de solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud.
S3KY	Clave de S3	El nombre de clave S3, sin incluir el nombre del bloque.

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 entregan.

Codificación	Campo	Descripción
AETM	Activar método	Método utilizado para deshabilitar la auditoría.
AEUN	Nombre de usuario	Nombre de usuario que ejecutó el comando para deshabilitar el registro de auditoría.
TRANSFORMACIÓN DIGITAL	Resultado	Este campo no tiene el valor NONE. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. NO SE utiliza NINGUNO en lugar de SUCS para que este mensaje no se filtre.

El mensaje implica que el registro se ha habilitado previamente, pero ahora se ha desactivado. Normalmente, este se utiliza solo durante la ingesta masiva con el fin de mejorar el rendimiento del sistema. Tras la actividad masiva, se restaura la auditoría (SADE) y la capacidad para desactivar la auditoría se bloquea de forma permanente.

SADE: Activación 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 vuelven a recopilar y entregar.

Codificación	Campo	Descripción
AETM	Activar método	Método utilizado para activar la auditoría.
AEUN	Nombre de usuario	Nombre de usuario que ejecutó el comando para habilitar el registro de auditoría.
TRANSFORMACIÓN DIGITAL	Resultado	Este campo no tiene el valor NONE. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. NO SE utiliza NINGUNO en lugar de SUCS para que este mensaje no se filtre.

El mensaje implica que el registro se ha desactivado previamente (SADD), pero ahora se ha restaurado. Normalmente, solo se utiliza durante la ingesta masiva con el fin de mejorar el rendimiento del sistema. Tras la actividad masiva, se restauran las auditorías y se bloquea de forma permanente la capacidad para deshabilitar la auditoría.

SCMT: Confirmación del almacén de objetos

El contenido de la cuadrícula no está disponible ni se reconoce como almacenado hasta que se ha cometido (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 genera cuando un bloque de contenido se confirma en el almacenamiento.

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido comprometido con el almacenamiento permanente.
TRANSFORMACIÓN DIGITAL	Código de resultado	Estado en el momento en que el objeto se almacenó en disco: SUCS: Objeto almacenado correctamente.

Este mensaje significa que se ha almacenado y verificado completamente un bloque de contenido dado y que ahora se puede solicitar. Se puede utilizar para realizar un seguimiento del flujo de datos dentro del sistema.

SDEL: ELIMINACIÓN DE S3

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

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0. Las operaciones en los depósitos no incluyen este campo.
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP de control de coherencia, si está presente en la solicitud.
CNID	Identificador de conexión	Identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño de contenido	El tamaño del objeto eliminado en bytes. Las operaciones en los depósitos no incluyen este campo.
DMRK	Eliminar ID de versión del marcador	El código de versión del marcador de borrado creado al eliminar un objeto de un bloque con versiones. Las operaciones en los depósitos no incluyen este campo.
GFID	ID de conexión de federación de grid	El ID de conexión de la conexión de federación de grid asociada con una solicitud de eliminación de replicación entre grid. Solo se incluyen en los registros de auditoría en el grid de destino.
GFSA	ID de cuenta de origen de federación de grid	El ID de cuenta del inquilino en la cuadrícula de origen para una solicitud de eliminación de replicación entre grid. Solo se incluyen en los registros de auditoría en el grid de destino.
HTRH	Encabezado de solicitud HTTP	<p>Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p><code>`X-Forwarded-For`</code> se incluye automáticamente si está presente en la solicitud y si la <code>`X-Forwarded-For`</code> El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p> </div> <p><code>x-amz-bypass-governance-retention</code> se incluye automáticamente si está presente en la solicitud.</p>
MTME	Hora de la última modificación	La Marca de hora de Unix, en microsegundos, indica cuándo se modificó por última vez el objeto.
TRANSFORMACIÓN DIGITAL	Código de resultado	Resultado de la transacción DE ELIMINACIÓN. El resultado es siempre: SUCS: Exitoso

Codificación	Campo	Descripción
S3AI	ID de cuenta de inquilino de S3 (remitente de solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de solicitudes)	El ID de clave de acceso de S3 hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Bloque de S3	El nombre de bloque de S3.
S3KY	Clave de S3	El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo.
S3SR	Subrecurso de S3	El bloque o subrecurso de objeto en el que se opera, si procede.
SACC	Nombre de cuenta de inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas.
SAIP	Dirección IP (remitente de solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de cuenta de inquilino de S3 (propietario del bloque)	El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del bloque)	El ID de cuenta de inquilino del propietario del bloque de destino. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
SGRP	Planta (grupo)	Si está presente, el objeto se eliminó en el sitio especificado, que no es el sitio donde se ingirió el objeto.

Codificación	Campo	Descripción
SUSR	URN de usuario de S3 (remitente de solicitudes)	El ID de cuenta de arrendatario y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vacío para solicitudes anónimas.
TIEMPO	Tiempo	Tiempo de procesamiento total de la solicitud en microsegundos.
TLIP	Dirección IP del equilibrador de carga de confianza	Si la solicitud se enrutó por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
VSID	ID de versión	El código de versión de la versión específica de un objeto que se eliminó. Las operaciones en cubos y objetos en depósitos sin versiones no incluyen este campo.

SGET: S3 GET

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

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

Codificación	Campo	Descripción
HTRH	Encabezado de solicitud HTTP	<p>Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p>`X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si la `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p> </div>
SONÓ	Lectura de rango	Solo para operaciones de lectura de rango. Indica el rango de bytes que se ha leído en esta solicitud. El valor después de la barra inclinada (/) muestra el tamaño de todo el objeto.
TRANSFORMACIÓN DIGITAL	Código de resultado	<p>Resultado DE LA transacción GET. El resultado es siempre:</p> <p>SUCS: Exitoso</p>
S3AI	ID de cuenta de inquilino de S3 (remitente de solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de solicitudes)	El ID de clave de acceso de S3 hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Bloque de S3	El nombre de bloque de S3.
S3KY	Clave de S3	El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo.
S3SR	Subrecurso de S3	El bloque o subrecurso de objeto en el que se opera, si procede.
SACC	Nombre de cuenta de inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas.
SAIP	Dirección IP (remitente de solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.

Codificación	Campo	Descripción
SBAC	Nombre de cuenta de inquilino de S3 (propietario del bloque)	El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del bloque)	El ID de cuenta de inquilino del propietario del bloque de destino. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
SUSR	URN de usuario de S3 (remitente de solicitudes)	El ID de cuenta de arrendatario y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vacío para solicitudes anónimas.
TIEMPO	Tiempo	Tiempo de procesamiento total de la solicitud en microsegundos.
TLIP	Dirección IP del equilibrador de carga de confianza	Si la solicitud se enrutó por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
VSID	ID de versión	El código de versión de la versión específica de un objeto que se solicitó. Las operaciones en cubos y objetos en depósitos sin versiones no incluyen este campo.

SHEA: CABEZA S3

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

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0. Las operaciones en los depósitos no incluyen este campo.
CNID	Identificador de conexión	Identificador único del sistema para la conexión TCP/IP.

Codificación	Campo	Descripción
CSIZ	Tamaño de contenido	El tamaño del objeto verificado en bytes. Las operaciones en los depósitos no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	<p>Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p><code>`X-Forwarded-For`</code> se incluye automáticamente si está presente en la solicitud y si la <code>`X-Forwarded-For`</code> El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p> </div>
TRANSFORMACIÓN DIGITAL	Código de resultado	<p>Resultado DE LA transacción GET. El resultado es siempre:</p> <p>SUCS: Exitoso</p>
S3AI	ID de cuenta de inquilino de S3 (remitente de solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de solicitudes)	El ID de clave de acceso de S3 hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Bloque de S3	El nombre de bloque de S3.
S3KY	Clave de S3	El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo.
SACC	Nombre de cuenta de inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas.
SAIP	Dirección IP (remitente de solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.

Codificación	Campo	Descripción
SBAC	Nombre de cuenta de inquilino de S3 (propietario del bloque)	El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del bloque)	El ID de cuenta de inquilino del propietario del bloque de destino. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
SUSR	URN de usuario de S3 (remitente de solicitudes)	El ID de cuenta de arrendatario y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vacío para solicitudes anónimas.
TIEMPO	Tiempo	Tiempo de procesamiento total de la solicitud en microsegundos.
TLIP	Dirección IP del equilibrador de carga de confianza	Si la solicitud se enrutó por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
VSID	ID de versión	El código de versión de la versión específica de un objeto que se solicitó. Las operaciones en cubos y objetos en depósitos sin versiones no incluyen este campo.

SPOS: PUBLICACIÓN DE S3

Cuando un cliente S3 emite una solicitud DE OBJETO POST, el servidor emite este mensaje si la transacción se realiza correctamente.

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0.
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP de control de coherencia, si está presente en la solicitud.

Codificación	Campo	Descripción
CNID	Identificador de conexión	Identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño de contenido	El tamaño del objeto recuperado en bytes.
HTRH	Encabezado de solicitud HTTP	<p>Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <pre>`X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si la `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</pre> </div> <p>(No se espera para SPOS).</p>
TRANSFORMACIÓN DIGITAL	Código de resultado	<p>Resultado de la solicitud DE restauración DE objetos POSTERIOR. El resultado es siempre:</p> <p>SUCS: Exitoso</p>
S3AI	ID de cuenta de inquilino de S3 (remitente de solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de solicitudes)	El ID de clave de acceso de S3 hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Bloque de S3	El nombre de bloque de S3.
S3KY	Clave de S3	El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo.
S3SR	Subrecurso de S3	<p>El bloque o subrecurso de objeto en el que se opera, si procede.</p> <p>Establezca «seleccionados» para una operación de selección de S3.</p>

Codificación	Campo	Descripción
SACC	Nombre de cuenta de inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas.
SAIP	Dirección IP (remitente de solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de cuenta de inquilino de S3 (propietario del bloque)	El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del bloque)	El ID de cuenta de inquilino del propietario del bloque de destino. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
SRCF	Configuración del subrecurso	Restaurar información.
SUSR	URN de usuario de S3 (remitente de solicitudes)	El ID de cuenta de arrendatario 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 de procesamiento total de la solicitud en microsegundos.
TLIP	Dirección IP del equilibrador de carga de confianza	Si la solicitud se enrutó por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
VSID	ID de versión	El código de versión de la versión específica de un objeto que se solicitó. Las operaciones en cubos y objetos en depósitos sin versiones no incluyen este campo.

SPUT: S3 PUT

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 cubo/objeto. El servidor emite este mensaje si la transacción se realiza correctamente.

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0. Las operaciones en los depósitos no incluyen este campo.
CMPS	Configuración de cumplimiento de normativas	La configuración de cumplimiento utilizada al crear el depósito, si está presente en la solicitud PUT Bucket (truncada a los primeros 1024 caracteres).
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP de control de coherencia, si está presente en la solicitud.
CNID	Identificador de conexión	Identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño de contenido	El tamaño del objeto recuperado en bytes. Las operaciones en los depósitos no incluyen este campo.
GFID	ID de conexión de federación de grid	El ID de conexión de la conexión de federación de grid asociada con una solicitud PUT DE replicación entre grid. Solo se incluyen en los registros de auditoría en el grid de destino.
GFSA	ID de cuenta de origen de federación de grid	El ID de cuenta del inquilino en la cuadrícula de origen para una solicitud de PUT DE replicación entre grid. Solo se incluyen en los registros de auditoría en el grid de destino.
HTRH	Encabezado de solicitud HTTP	<p>Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"><p><code>`X-Forwarded-For`</code> se incluye automáticamente si está presente en la solicitud y si la <code>`X-Forwarded-For`</code> El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p></div> <p><code>x-amz-bypass-governance-retention</code> se incluye automáticamente si está presente en la solicitud.</p>

Codificación	Campo	Descripción
LKEN	Bloqueo de objeto activado	Valor de la cabecera de la solicitud <code>x-amz-bucket-object-lock-enabled</code> , Si está presente en la solicitud PUT Bucket.
LKLH	Bloqueo de objeto retención legal	Valor de la cabecera de la solicitud <code>x-amz-object-lock-legal-hold</code> , Si está presente en la solicitud PONER objeto.
LKMD	Modo de retención de bloqueo de objetos	Valor de la cabecera de la solicitud <code>x-amz-object-lock-mode</code> , Si está presente en la solicitud PONER objeto.
LKRU	Bloqueo de objeto mantener hasta la fecha	Valor de la cabecera de la solicitud <code>x-amz-object-lock-retain-until-date</code> , Si está presente en la solicitud PONER objeto.
MTME	Hora de la última modificación	La Marca de hora de Unix, en microsegundos, indica cuándo se modificó por última vez el objeto.
TRANSFORMACIÓN DIGITAL	Código de resultado	Resultado de la transacción PUT. El resultado es siempre: SUCS: Exitoso
S3AI	ID de cuenta de inquilino de S3 (remitente de solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de solicitudes)	El ID de clave de acceso de S3 hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Bloque de S3	El nombre de bloque de S3.
S3KY	Clave de S3	El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo.
S3SR	Subrecurso de S3	El bloque o subrecurso de objeto en el que se opera, si procede.
SACC	Nombre de cuenta de inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas.

Codificación	Campo	Descripción
SAIP	Dirección IP (remitente de solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de cuenta de inquilino de S3 (propietario del bloque)	El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del bloque)	El ID de cuenta de inquilino del propietario del bloque de destino. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
SRCF	Configuración del subrecurso	La nueva configuración del subrecurso (truncada a los primeros 1024 caracteres).
SUSR	URN de usuario de S3 (remitente de solicitudes)	El ID de cuenta de arrendatario y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vacío para solicitudes anónimas.
TIEMPO	Tiempo	Tiempo de procesamiento total de la solicitud en microsegundos.
TLIP	Dirección IP del equilibrador de carga de confianza	Si la solicitud se enrutó por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
ID	ID de carga	Sólo se incluye en los mensajes SPUT para operaciones de carga de varias partes completas. 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 código de versión de un nuevo objeto creado en un bloque con versiones. Las operaciones en cubos y objetos en depósitos sin versiones no incluyen este campo.
VSST	Estado de control de versiones	El nuevo estado de creación de versiones de un bloque. Se utilizan dos estados: "Activado" o "Suspendido". Las operaciones en objetos no incluyen este campo.

SREM: Almacén de objetos Quitar

Este mensaje se genera cuando se elimina el contenido del almacenamiento persistente y ya no se puede acceder a él mediante API habituales.

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido eliminado del almacenamiento permanente.
TRANSFORMACIÓN DIGITAL	Código de resultado	Indica el resultado de las operaciones de eliminación de contenido. El único valor definido es: ÉXITO: Contenido eliminado del almacenamiento persistente

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

SUPD: Se han actualizado metadatos S3

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

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0. Las operaciones en los depósitos no incluyen este campo.
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP de control de coherencia, si está presente en la solicitud, al actualizar la configuración de cumplimiento de un bloque.
CNID	Identificador de conexión	Identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño de contenido	El tamaño del objeto recuperado en bytes. Las operaciones en los depósitos no incluyen este campo.

Codificación	Campo	Descripción
HTRH	Encabezado de solicitud HTTP	<p>Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p>`X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si la `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p> </div>
TRANSFORMACIÓN DIGITAL	Código de resultado	<p>Resultado DE LA transacción GET. El resultado es siempre:</p> <p>SUCS: Exitoso</p>
S3AI	ID de cuenta de inquilino de S3 (remitente de solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de solicitudes)	El ID de clave de acceso de S3 hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Bloque de S3	El nombre de bloque de S3.
S3KY	Clave de S3	El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo.
SACC	Nombre de cuenta de inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas.
SAIP	Dirección IP (remitente de solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de cuenta de inquilino de S3 (propietario del bloque)	El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.

Codificación	Campo	Descripción
SBAI	ID de cuenta de inquilino de S3 (propietario del bloque)	El ID de cuenta de inquilino del propietario del bloque de destino. Se utiliza para identificar el acceso de cuenta cruzada o anónimo.
SUSR	URN de usuario de S3 (remitente de solicitudes)	El ID de cuenta de arrendatario y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vacío para solicitudes anónimas.
TIEMPO	Tiempo	Tiempo de procesamiento total de la solicitud en microsegundos.
TLIP	Dirección IP del equilibrador de carga de confianza	Si la solicitud se enrutó por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
VSID	ID de versión	El código de versión de la versión específica de un objeto cuyos metadatos se han actualizado. Las operaciones en cubos y objetos en depósitos sin versiones no incluyen este campo.

SVRF: Fallo de verificación del almacén de objetos

Este mensaje se emite siempre que un bloque de contenido falla en el proceso de verificación. Cada vez que se leen los datos de objetos replicados o se escriben en el disco, se realizan varias comprobaciones de verificación e integridad para garantizar que los datos enviados al usuario solicitante sean idénticos a los datos procesados originalmente en el sistema. Si alguna de estas comprobaciones falla, el sistema pone automáticamente en cuarentena los datos de objeto replicados corruptos para impedir que se recupere de nuevo.

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido que ha fallado la verificación.

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Código de resultado	<p>Tipo de fallo de verificación:</p> <p>CRCF: Error en la comprobación de redundancia cíclica (CRC).</p> <p>HMAC: Error en la comprobación del código de autenticación de mensajes basados en hash (HMAC).</p> <p>EHS: Hash de contenido cifrado inesperado.</p> <p>PHS: Hash de contenido original inesperado.</p> <p>SEQC: Secuencia de datos incorrecta en el disco.</p> <p>PERR: Estructura no válida del archivo de disco.</p> <p>DERR: Error de disco.</p> <p>FNAM: Nombre de archivo incorrecto.</p>



Este mensaje debe supervisarse de cerca. Los fallos de verificación de contenido pueden indicar fallos de hardware inminentes.

Para determinar qué operación ha activado el mensaje, consulte el valor del campo AMID (ID del módulo). Por ejemplo, un valor de SVAFY indica que el mensaje fue generado por el módulo de verificador de almacenamiento, es decir, la verificación en segundo plano y STOR indica que el mensaje se ha activado mediante la recuperación de contenido.

SVRU: Verificación del almacén de objetos desconocida

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

Codificación	Campo	Descripción
FPTH	Ruta del archivo	Ruta de acceso del archivo de la copia de objeto inesperada.
TRANSFORMACIÓN DIGITAL	Resultado	Este campo tiene el valor 'NONE'. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. 'NINGUNO' se utiliza en lugar de 'UCS' para que este mensaje no se filtre.



El mensaje de auditoría SVRU: Object Store Verify Unknown debe supervisarse de cerca. Significa que se han detectado 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 pueden indicar fallos de hardware inminentes.

SYSD: Parada del nodo

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

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Apagado limpio	La naturaleza del cierre: SUCS: El sistema se cerró correctamente.

El mensaje no indica si el servidor host se está parando, sólo el servicio de creación de informes. La RSLT de un SYSD no puede indicar un apagado “sucio”, porque el mensaje se genera solo mediante apagados “limpios”.

SYST: Nodo detenido

Cuando se detiene correctamente un servicio, este mensaje se genera para indicar que se ha solicitado el cierre 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 que se reinicia el servicio).

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Apagado limpio	La naturaleza del cierre: SUCS: El sistema se cerró correctamente.

El mensaje no indica si el servidor host se está parando, sólo el servicio de creación de informes. El código RSLT de un mensaje SYST no puede indicar un cierre “sucio”, porque el mensaje se genera solo mediante apagados “limpios”.

SYSU: Inicio del nodo

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

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	Apagado limpio	La naturaleza del cierre: SUCS: El sistema se cerró limpiamente. DSDN: El sistema no se ha apagado correctamente. VRGN: El sistema se inició por primera vez tras la instalación del servidor (o la reinstalación).

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

- Detectar discontinuidad en el seguimiento de auditoría.
- Determine si un servicio presenta errores durante el funcionamiento (ya que la naturaleza distribuida del sistema StorageGRID puede enmascarar estos fallos). El Administrador del servidor reinicia automáticamente un servicio fallido.

WDEL: ELIMINACIÓN de Swift

Cuando un cliente de Swift emite una transacción DE ELIMINACIÓN, se realiza una solicitud para quitar el objeto o contenedor especificado. El servidor emite este mensaje si la transacción se realiza correctamente.

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0. Las operaciones en contenedores no incluyen este campo.
CSIZ	Tamaño de contenido	El tamaño del objeto eliminado en bytes. Las operaciones en contenedores no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p><code>`X-Forwarded-For`</code> se incluye automáticamente si está presente en la solicitud y si la <code>`X-Forwarded-For`</code> El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p> </div>
MTME	Hora de la última modificación	La Marca de hora de Unix, en microsegundos, indica cuándo se modificó por última vez el objeto.
TRANSFORMACIÓN DIGITAL	Código de resultado	Resultado de la transacción DE ELIMINACIÓN. El resultado es siempre: SUCS: Exitoso
SAIP	Dirección IP del cliente solicitante	La dirección IP de la aplicación cliente que realizó la solicitud.
SGRP	Planta (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 de procesamiento total de la solicitud en microsegundos.

Codificación	Campo	Descripción
TLIP	Dirección IP del equilibrador de carga de confianza	Si la solicitud se enrutó por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
WACC	ID de cuenta de Swift	El ID de cuenta único especificado por el sistema StorageGRID.
WCON	Contenedor Swift	El nombre del contenedor Swift.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones en contenedores no incluyen este campo.
WUSR	Usuario de la cuenta de Swift	El nombre de usuario de la cuenta de Swift que identifica de manera exclusiva al cliente que realiza la transacción.

WGET: Swift GET

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

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0. Las operaciones en cuentas y contenedores no incluyen este campo.
CSIZ	Tamaño de contenido	El tamaño del objeto recuperado en bytes. Las operaciones en cuentas y contenedores no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p><code>`X-Forwarded-For`</code> se incluye automáticamente si está presente en la solicitud y si la <code>`X-Forwarded-For`</code> El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p> </div>

Codificación	Campo	Descripción
TRANSFORMACIÓN DIGITAL	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 de procesamiento total de la solicitud en microsegundos.
TLIP	Dirección IP del equilibrador de carga de confianza	Si la solicitud se enrutó por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
WACC	ID de cuenta de Swift	El ID de cuenta único especificado por el sistema StorageGRID.
WCON	Contenedor Swift	El nombre del contenedor Swift. Las operaciones en las cuentas no incluyen este campo.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones en cuentas y contenedores no incluyen este campo.
WUSR	Usuario de la cuenta de Swift	El nombre de usuario de la cuenta de Swift que identifica de manera exclusiva al cliente que realiza la transacción.

WHEA: CABEZA de Swift

Cuando un cliente de Swift emite una transacción HEAD, se realiza una solicitud para comprobar la existencia de una cuenta, un contenedor o un objeto, y recuperar los metadatos relevantes. El servidor emite este mensaje si la transacción se realiza correctamente.

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0. Las operaciones en cuentas y contenedores no incluyen este campo.
CSIZ	Tamaño de contenido	El tamaño del objeto recuperado en bytes. Las operaciones en cuentas y contenedores no incluyen este campo.

Codificación	Campo	Descripción
HTRH	Encabezado de solicitud HTTP	<p>Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p>`X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si la `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p> </div>
TRANSFORMACIÓN DIGITAL	Código de resultado	<p>Resultado de la transacción PRINCIPAL. El resultado es siempre:</p> <p>SUCS: Exitoso</p>
SAIP	Dirección IP del cliente solicitante	La dirección IP de la aplicación cliente que realizó la solicitud.
TIEMPO	Tiempo	Tiempo de procesamiento total de la solicitud en microsegundos.
TLIP	Dirección IP del equilibrador de carga de confianza	Si la solicitud se enrutó por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
WACC	ID de cuenta de Swift	El ID de cuenta único especificado por el sistema StorageGRID.
WCON	Contenedor Swift	El nombre del contenedor Swift. Las operaciones en las cuentas no incluyen este campo.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones en cuentas y contenedores no incluyen este campo.
WUSR	Usuario de la cuenta de Swift	El nombre de usuario de la cuenta de Swift que identifica de manera exclusiva al cliente que realiza la transacción.

WPUT: SWIFT PUT

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 se realiza correctamente.

Codificación	Campo	Descripción
CBID	Identificador de bloque de contenido	Identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0. Las operaciones en contenedores no incluyen este campo.
CSIZ	Tamaño de contenido	El tamaño del objeto recuperado en bytes. Las operaciones en contenedores no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración. <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p><code>`X-Forwarded-For`</code> se incluye automáticamente si está presente en la solicitud y si la <code>`X-Forwarded-For`</code> El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p> </div>
MTME	Hora de la última modificación	La Marca de hora de Unix, en microsegundos, indica cuándo se modificó por última vez el objeto.
TRANSFORMACIÓN DIGITAL	Código de resultado	Resultado de la transacción PUT. 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 de procesamiento total de la solicitud en microsegundos.
TLIP	Dirección IP del equilibrador de carga de confianza	Si la solicitud se enrutó por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
WACC	ID de cuenta de Swift	El ID de cuenta único especificado por el sistema StorageGRID.
WCON	Contenedor Swift	El nombre del contenedor Swift.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones en contenedores no incluyen este campo.

Codificación	Campo	Descripción
WUSR	Usuario de la cuenta de Swift	El nombre de usuario de la cuenta de Swift que identifica de manera exclusiva al cliente que realiza la transacción.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.