



Solucionar problemas de objetos y almacenamiento

StorageGRID 11.5

NetApp
April 11, 2024

Tabla de contenidos

- Solucionar problemas de objetos y almacenamiento..... 1
 - Confirmación de ubicaciones de datos de objeto 1
 - Errores del almacén de objetos (volumen de almacenamiento) 3
 - Verificando la integridad del objeto 4
 - Solución de problemas de datos de objetos perdidos o faltantes 11
 - Solución de problemas de la alerta de almacenamiento de datos de objeto Low 24
 - Solución de problemas de la alarma de estado de almacenamiento (SST) 26
 - Solución de problemas de la entrega de mensajes de servicios de la plataforma (alarma SMTT)..... 31

Solucionar problemas de objetos y almacenamiento

Existen varias tareas que puede realizar para determinar el origen de los problemas de objeto y almacenamiento.

Confirmación de ubicaciones de datos de objeto

En función del problema, es posible que desee confirmar dónde se almacenan los datos del objeto. Por ejemplo, puede que desee verificar que la política de ILM esté funcionando como se espera y que los datos de objetos se almacenen donde estaba previsto.

Lo que necesitará

- Debe tener un identificador de objeto, que puede ser uno de los siguientes:
 - **UUID:** Identificador único universal del objeto. Introduzca el UUID en toda la mayúscula.
 - **CBID:** Identificador único del objeto dentro de StorageGRID . Es posible obtener el CBID de un objeto del registro de auditoría. Introduzca el CBID en todas las mayúsculas.
 - **Bloque de S3 y clave de objeto:** Cuando un objeto se ingiere a través de la interfaz S3, la aplicación cliente utiliza una combinación de bucket y clave de objeto para almacenar e identificar el objeto.
 - **Nombre de objeto y contenedor Swift:** Cuando un objeto se ingiere a través de la interfaz Swift, la aplicación cliente utiliza una combinación de nombre de objeto y contenedor para almacenar e identificar el objeto.

Pasos

1. Seleccione **ILM > Búsqueda de metadatos de objetos**.
2. Escriba el identificador del objeto en el campo **Identificador**.

Es posible introducir un UUID, CBID, bucket/object-key de S3 o nombre de objeto/contenedor de Swift.

Object Metadata Lookup

Enter the identifier for any object stored in the grid to view its metadata.

Identifier

Look Up

3. Haga clic en **Buscar**.

Se muestran los resultados de la búsqueda de metadatos de los objetos. Esta página incluye los siguientes tipos de información:

- Metadatos del sistema, incluidos el ID de objeto (UUID), el nombre del objeto, el nombre del contenedor, el ID o el nombre de la cuenta de inquilino, el tamaño lógico del objeto, la fecha y hora en que se creó el objeto por primera vez, y la fecha y hora en que se modificó por última vez el objeto.
- Todos los pares de valor de clave de metadatos de usuario personalizados asociados con el objeto.
- Para los objetos S3, cualquier par de etiqueta de objeto clave-valor asociado al objeto.

- Para las copias de objetos replicadas, la ubicación de almacenamiento actual de cada copia.
- Para las copias de objetos codificados de borrado, la ubicación actual de almacenamiento de cada fragmento.
- Para las copias de objetos en un Cloud Storage Pool, la ubicación del objeto, incluido el nombre del bloque externo y el identificador único del objeto.
- Para objetos segmentados y objetos multipartes, una lista de segmentos de objetos que incluyen identificadores de segmentos y tamaños de datos. Para objetos con más de 100 segmentos, sólo se muestran los primeros 100 segmentos.
- Todos los metadatos del objeto en el formato de almacenamiento interno sin procesar. Estos metadatos sin procesar incluyen los metadatos internos del sistema que no se garantiza que continúen del lanzamiento al lanzamiento.

En el ejemplo siguiente se muestran los resultados de búsqueda de metadatos de objetos para un objeto de prueba S3 almacenado como dos copias replicadas.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x88230E7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAWS": "2",

```

Información relacionada

"Gestión de objetos con ILM"

"Use S3"

"Use Swift"

Errores del almacén de objetos (volumen de almacenamiento)

El almacenamiento subyacente en un nodo de almacenamiento se divide en almacenes de objetos. Estos almacenes de objetos son particiones físicas que actúan como puntos de montaje para el almacenamiento del sistema StorageGRID. Los almacenes de objetos también se conocen como volúmenes de almacenamiento.

Es posible ver la información de almacén de objetos de cada nodo de almacenamiento. Los almacenes de objetos se muestran en la parte inferior de la página **Nodes > Storage Node > Storage**.

Disk Devices						
Name	World Wide Name	I/O Load	Read Rate	Write Rate		
croot(8:1,sda1)	N/A	1.62%	0 bytes/s	177 KB/s		
cvloc(8:2,sda2)	N/A	17.28%	0 bytes/s	2 MB/s		
sdc(8:16,sdb)	N/A	0.00%	0 bytes/s	11 KB/s		
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	0 bytes/s		
sds(8:48,sdd)	N/A	0.00%	0 bytes/s	0 bytes/s		

Volumes						
Mount Point	Device	Status	Size	Available	Write Cache Status	
/	croot	Online	21.00 GB	14.25 GB		Unknown
/var/local	cvloc	Online	85.86 GB	84.39 GB		Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.18 GB		Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB		Enabled
/var/local/rangedb/2	sds	Online	107.32 GB	107.18 GB		Enabled

Object Stores						
ID	Size	Available	Replicated Data	EC Data	Object Data (%)	Health
0000	107.32 GB	96.45 GB	994.37 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Para ver más detalles sobre cada nodo de almacenamiento, siga estos pasos:

1. Seleccione **Soporte > Herramientas > Topología de cuadrícula**.
2. Seleccione **site > Storage Node > LDR > Storage > Overview > Main**.



Overview: LDR (DC1-S1) - Storage

Updated: 2020-01-29 15:03:39 PST

Storage State - Desired:	Online	
Storage State - Current:	Online	
Storage Status:	No Errors	

Utilization

Total Space:	322 GB	
Total Usable Space:	311 GB	
Total Usable Space (Percent):	96.534 %	
Total Data:	994 KB	
Total Data (Percent):	0 %	

Replication

Block Reads:	0	
Block Writes:	0	
Objects Retrieved:	0	
Objects Committed:	0	
Objects Deleted:	0	
Delete Service State:	Enabled	

Object Store Volumes

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health
0000	107 GB	96.4 GB	994 KB	0 B	0.001 %	No Errors
0001	107 GB	107 GB	0 B	0 B	0 %	No Errors
0002	107 GB	107 GB	0 B	0 B	0 %	No Errors

En función de la naturaleza del fallo, los fallos con un volumen de almacenamiento pueden reflejarse en una alarma del estado del almacenamiento o del estado de un almacén de objetos. Si un volumen de almacenamiento falla, debe reparar el volumen de almacenamiento con errores para restaurar el nodo de almacenamiento a Lo antes posible. con todas las funcionalidades. Si es necesario, puede ir a la ficha **Configuración** y colocar el nodo de almacenamiento en un estado de sólo lectura-para que el sistema StorageGRID pueda utilizarlo para la recuperación de datos mientras se prepara para una recuperación completa del servidor.

Información relacionada

["Mantener recuperar"](#)

Verificando la integridad del objeto

El sistema StorageGRID verifica la integridad de los datos de objetos en los nodos de almacenamiento y comprueba si hay objetos dañados o ausentes.

Hay dos procesos de verificación: Verificación de fondo y verificación en primer plano. Trabajan conjuntamente para garantizar la integridad de los datos. La verificación en segundo plano se ejecuta automáticamente y comprueba continuamente la corrección de los datos del objeto. Un usuario puede activar la verificación en primer plano para verificar más rápidamente la existencia (aunque no la corrección) de objetos.

Qué es la verificación de antecedentes

El proceso de verificación en segundo plano comprueba de forma automática y continua si hay copias dañadas de los datos de los objetos e intenta reparar automáticamente los problemas que encuentre.

La verificación en segundo plano comprueba la integridad de los objetos replicados y los objetos codificados mediante borrado de la siguiente manera:

- **Objetos replicados:** Si el proceso de verificación en segundo plano encuentra un objeto replicado que está dañado, la copia dañada se quita de su ubicación y se pone en cuarentena en otro lugar del nodo de almacenamiento. A continuación, se genera y coloca una copia nueva sin daños para satisfacer la política activa de ILM. Es posible que la nueva copia no se coloque en el nodo de almacenamiento que se utilizó para la copia original.



Los datos de objetos dañados se ponen en cuarentena en lugar de eliminarse del sistema, de modo que aún se puede acceder a ellos. Para obtener más información sobre el acceso a los datos de objetos en cuarentena, póngase en contacto con el soporte técnico.

- **Objetos codificados con borrado:** Si el proceso de verificación en segundo plano detecta que un fragmento de un objeto codificado con borrado está dañado, StorageGRID intenta automáticamente reconstruir el fragmento que falta en el mismo nodo de almacenamiento, utilizando los fragmentos restantes de datos y paridad. Si el fragmento dañado no se puede reconstruir, el atributo copias dañadas detectadas (ECOR) aumenta en uno y se intenta recuperar otra copia del objeto. Si la recuperación se realiza correctamente, se realiza una evaluación de ILM para crear una copia de reemplazo del objeto codificado por borrado.

El proceso de verificación en segundo plano comprueba los objetos solo en los nodos de almacenamiento. No comprueba los objetos en los nodos de archivado ni en un pool de almacenamiento en cloud. Los objetos deben tener una antigüedad superior a cuatro días para poder optar a la verificación en segundo plano.

La verificación en segundo plano se ejecuta a una velocidad continua diseñada para no interferir con las actividades normales del sistema. No se puede detener la verificación en segundo plano. Sin embargo, puede aumentar la tasa de verificación en segundo plano para verificar más rápidamente el contenido de un nodo de almacenamiento si sospecha que existe un problema.

Alertas y alarmas (heredadas) relacionadas con la verificación en segundo plano

Si el sistema detecta un objeto dañado que no puede corregir automáticamente (debido a que el daño impide que el objeto se identifique), se activa la alerta **objeto dañado no identificado**.

Si la verificación en segundo plano no puede reemplazar un objeto dañado porque no puede localizar otra copia, se activan la alarma **objetos perdidos** y la alarma heredada PERDIDA (objetos perdidos).

Modificación de la tasa de verificación en segundo plano

Puede cambiar la velocidad a la que la verificación en segundo plano comprueba los datos de objetos replicados en un nodo de almacenamiento si tiene dudas acerca de la integridad de los datos.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

Es posible cambiar la tasa de verificación para la verificación en segundo plano en un nodo de almacenamiento:

- **Adaptive:** Ajuste predeterminado. La tarea está diseñada para verificar un máximo de 4 MB/s o 10 objetos/s (lo que se supere primero).
- **Alto:** La verificación del almacenamiento procede rápidamente, a un ritmo que puede ralentizar las actividades normales del sistema.


Utilice la alta tasa de verificación sólo cuando sospeche que un error de hardware o software puede tener datos de objeto dañados. Una vez finalizada la verificación en segundo plano de prioridad alta, la velocidad de verificación se restablece automáticamente a adaptable.

Pasos

1. Seleccione **Soporte > Herramientas > Topología de cuadrícula**.
2. Seleccione **Storage Node > LDR > Verification**.
3. Seleccione **Configuración > Principal**.
4. Vaya a **LDR > verificación > Configuración > Principal**.
5. En verificación de fondo, seleccione **velocidad de verificación > Alta** o **velocidad de verificación > adaptable**.

Overview Alarms Reports Configuration

Main Alarms

 Configuration: LDR (DC2-S1-106-147) - Verification
Updated: 2019-04-24 16:13:44 PDT

Reset Missing Objects Count

Foreground Verification

ID	Verify
0	<input type="checkbox"/>
1	<input type="checkbox"/>
2	<input type="checkbox"/>


Background Verification

Verification Rate

Reset Corrupt Objects Count

Quarantined Objects

Delete Quarantined Objects

Apply Changes 



Al establecer la velocidad de verificación en Alta se activa la alarma heredada de VPRI (tasa de verificación) en el nivel de aviso.

1. Haga clic en **aplicar cambios**.
2. Supervise los resultados de la verificación en segundo plano de los objetos replicados.
 - a. Vaya a **Nodes > Storage Node > Objects**.
 - b. En la sección verificación, supervise los valores de **objetos corruptos** y **objetos corruptos no identificados**.

Si la verificación en segundo plano encuentra datos de objeto replicados dañados, se incrementa la métrica **objetos corruptos** y StorageGRID intenta extraer el identificador de objeto de los datos, de la siguiente manera:

- Si se puede extraer el identificador del objeto, StorageGRID crea automáticamente una nueva copia de los datos del objeto. La nueva copia puede realizarse en cualquier punto del sistema StorageGRID que satisfaga la política de ILM activa.
 - Si no se puede extraer el identificador de objeto (porque ha estado dañado), se incrementa la métrica **objetos corruptos no identificados** y se activa la alerta **objeto dañado no identificado**.
- c. Si se encuentran datos de objeto replicado dañados, póngase en contacto con el soporte técnico para determinar la causa raíz de los daños.
3. Supervise los resultados de la verificación en segundo plano para objetos codificados mediante borrado.

Si la verificación en segundo plano encuentra fragmentos dañados de datos de objeto codificados con borrado, se incrementa el atributo fragmentos dañados detectados. StorageGRID se recupera al reconstruir el fragmento dañado in situ en el mismo nodo de almacenamiento.

- a. Seleccione **Soporte > Herramientas > Topología de cuadrícula**.
 - b. Seleccione **Storage Node > LDR > Código de borrado**.
 - c. En la tabla resultados de verificación, supervise el atributo fragmentos dañados detectados (ECCD).
4. Una vez que el sistema StorageGRID restaura automáticamente los objetos dañados, restablece el número de objetos dañados.
 - a. Seleccione **Soporte > Herramientas > Topología de cuadrícula**.
 - b. Seleccione **Storage Node > LDR > Verification > Configuration**.
 - c. Seleccione **Restablecer recuento de objetos dañados**.
 - d. Haga clic en **aplicar cambios**.
 5. Si está seguro de que los objetos en cuarentena no son necesarios, puede eliminarlos.



Si se activó la alerta **objetos perdidos** o la alarma heredada PERDIDA (objetos perdidos), es posible que el soporte técnico desee tener acceso a los objetos en cuarentena para ayudar a depurar el problema subyacente o intentar recuperar datos.

1. Seleccione **Soporte > Herramientas > Topología de cuadrícula**.
2. Seleccione **Storage Node > LDR > Verification > Configuration**.
3. Seleccione **Eliminar objetos en cuarentena**.
4. Haga clic en **aplicar cambios**.

Qué es la verificación en primer plano

La verificación en primer plano es un proceso iniciado por el usuario que comprueba si todos los datos de

objeto esperados existen en un nodo de almacenamiento. La verificación en primer plano se utiliza para verificar la integridad de un dispositivo de almacenamiento.

La verificación en primer plano es una alternativa más rápida a la verificación en segundo plano que comprueba la existencia, pero no la integridad, de datos de objetos en un nodo de almacenamiento. Si la verificación en primer plano encuentra que faltan muchos elementos, puede que haya un problema con todo o parte de un dispositivo de almacenamiento asociado al nodo de almacenamiento.

La verificación en primer plano comprueba tanto los datos de objeto replicados como los de objeto con código de borrado como los siguientes:

- **Objetos replicados:** Si falta una copia de los datos del objeto replicado, StorageGRID intenta automáticamente sustituir la copia de las copias almacenadas en otro lugar del sistema. El nodo de almacenamiento ejecuta una copia existente a través de una evaluación de ILM, que determina que ya no se cumple la política actual de ILM para este objeto, ya que la copia que falta ya no existe en la ubicación esperada. Se genera una copia nueva y se coloca para satisfacer la política de ILM activa del sistema. Es posible que esta nueva copia no se coloque en la misma ubicación en la que se guardó la copia que falta.
- **Objetos codificados con borrado:** Si falta un fragmento de un objeto codificado con borrado, StorageGRID intenta automáticamente reconstruir el fragmento que falta en el mismo nodo de almacenamiento utilizando los fragmentos restantes. Si el fragmento que falta no se puede reconstruir (porque se han perdido demasiados fragmentos), el atributo copias dañadas detectadas (ECOR) aumenta en uno. A continuación, ILM intenta encontrar otra copia del objeto, que puede usar para generar una nueva copia codificada por borrado.

Si la verificación en primer plano identifica un problema con la codificación de borrado en un volumen de almacenamiento, la tarea de verificación en primer plano se suspende con un mensaje de error que identifica el volumen afectado. Debe realizar un procedimiento de recuperación de todos los volúmenes de almacenamiento afectados.

Si no se encuentran otras copias de un objeto replicado que falta o un objeto dañado con código de borrado en la cuadrícula, se activan la alerta **objetos perdidos** y la alarma heredada PERDIDA (objetos perdidos).

Ejecutando verificación en primer plano

La verificación en primer plano le permite verificar la existencia de datos en un nodo de almacenamiento. Los datos de objeto ausentes pueden indicar que existe un problema con el dispositivo de almacenamiento subyacente.

Lo que necesitará

- Debe asegurarse de que no se estén ejecutando las siguientes tareas de cuadrícula:
 - Expansión de cuadrícula: Agregar servidor (GEXP) al agregar un nodo de almacenamiento
 - Retirada del nodo de almacenamiento (LDCM) en el mismo nodo de almacenamiento Si estas tareas de cuadrícula están en ejecución, espere a que finalice o libere su bloqueo.
- Se aseguró de que el almacenamiento esté en línea. (Seleccione **Soporte > Herramientas > Topología de cuadrícula**. A continuación, seleccione **Storage Node > LDR > Storage > Overview > Main**. Asegúrese de que **Estado de almacenamiento - corriente** está en línea.)
- Comprobó que los siguientes procedimientos de recuperación no se están ejecutando en el mismo nodo de almacenamiento:
 - Recuperación de un volumen de almacenamiento con fallos
 - Recuperación de un nodo de almacenamiento con un error en la verificación primer plano de la unidad del sistema no proporciona información útil mientras los procedimientos de recuperación están en

curso.

Acerca de esta tarea

La verificación en primer plano busca los datos del objeto replicado que faltan y los datos del objeto con código de borrado que faltan:

- Si la verificación en primer plano encuentra grandes cantidades de datos de objetos que faltan, es probable que haya un problema con el almacenamiento del nodo de almacenamiento que se deba investigar y solucionar.
- Si la verificación en primer plano encuentra un error de almacenamiento asociado con datos codificados de borrado, lo notificará. Debe realizar una recuperación del volumen de almacenamiento para reparar el error.

Puede configurar la verificación en primer plano para comprobar todos los almacenes de objetos de un nodo de almacenamiento o sólo los almacenes de objetos específicos.

Si la verificación en primer plano encuentra datos de objeto que faltan, el sistema StorageGRID intenta reemplazarlo. Si no se puede hacer una copia de reemplazo, puede activarse la alarma PÉRDIDA (objetos perdidos).

La verificación en primer plano genera una tarea de cuadrícula verificación en primer plano de LDR que, en función del número de objetos almacenados en un nodo de almacenamiento, puede tardar días o semanas en completarse. Es posible seleccionar varios nodos de almacenamiento al mismo tiempo; sin embargo, estas tareas de grid no se ejecutan simultáneamente. En su lugar, se ponen en cola y se ejecutan una después de la otra hasta que finalice. Cuando la verificación en primer plano está en curso en un nodo de almacenamiento, no puede iniciar otra tarea de verificación en primer plano en ese mismo nodo de almacenamiento aunque la opción de verificar volúmenes adicionales pueda parecer estar disponible para el nodo de almacenamiento.


Si un nodo de almacenamiento distinto del que se está ejecutando la verificación en primer plano se desconecta, la tarea de cuadrícula continúa ejecutándose hasta que el atributo **% completado** alcance el 99.99%. A continuación, el atributo **% completado** vuelve al 50% y espera a que el nodo de almacenamiento vuelva al estado en línea. Cuando el estado del nodo de almacenamiento vuelve a estar en línea, la tarea de cuadrícula verificación de primer plano LDR continúa hasta que se completa.

Pasos

1. Seleccione **Storage Node > LDR > Verification**.
2. Seleccione **Configuración > Principal**.
3. En **verificación de primer plano**, seleccione la casilla de verificación de cada ID de volumen de almacenamiento que desee verificar.

Overview Alarms Reports **Configuration**

Main Alarms

 **Configuration: LDR (dc1-cs1-99-82) - Verification**
Updated: 2015-08-19 14:07:04 PDT

Reset Missing Objects Count


Foreground Verification

ID	Verify
0	<input checked="" type="checkbox"/>
1	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>

Background Verification

Verification Rate

Reset Corrupt Objects Count

Apply Changes 

4. Haga clic en **aplicar cambios**.

Espere a que la página se actualice y se recargará automáticamente antes de salir de la página. Una vez actualizados, los almacenes de objetos dejan de estar disponibles para su selección en ese nodo de almacenamiento.

Se genera una tarea de cuadrícula verificación de primer plano de LDR y se ejecuta hasta que se completa, se detiene o se cancela.

5. Supervisar los objetos que faltan o los fragmentos que faltan:

a. Seleccione **Storage Node > LDR > Verification**.

b. En la ficha Descripción general en **resultados de verificación**, anote el valor de **objetos perdidos**.

Nota: El mismo valor se informa como **objetos perdidos** en la página Nodes. Vaya a **Nodes > Storage Node** y seleccione la ficha **objetos**.

Si el número de **objetos ausentes detectados** es grande (si faltan cientos de objetos), es probable que haya un problema con el almacenamiento del nodo de almacenamiento. Póngase en contacto con el soporte técnico.

c. Seleccione **Storage Node > LDR > código de borrado**.

d. En la ficha Descripción general en **resultados de verificación**, anote el valor de **fragmentos ausentes detectados**.

Si el número de **fragmentos ausentes detectados** es grande (si faltan cientos de fragmentos), es probable que haya un problema con el almacenamiento del nodo de almacenamiento. Póngase en

contacto con el soporte técnico.

Si la verificación en primer plano no detecta un número importante de copias de objetos replicados que faltan o un número importante de fragmentos, el almacenamiento funciona con normalidad.

6. Supervise la finalización de la tarea de la cuadrícula de verificación en primer plano:
 - a. Seleccione **Soporte > Herramientas > Topología de cuadrícula**. A continuación, seleccione **site > Admin Node > CMN > Grid Task > Overview > Main**.
 - b. Compruebe que la tarea de la cuadrícula de verificación en primer plano está progresando sin errores.

Nota: Se activa una alarma de nivel de aviso en el estado de la tarea de la cuadrícula (SCAS) si la tarea de la cuadrícula de verificación en primer plano se detiene.

- c. Si la tarea de la cuadrícula se detiene con un `critical storage error`, recupere el volumen afectado y, a continuación, ejecute la verificación en primer plano en los volúmenes restantes para comprobar si hay errores adicionales.

Atención: Si la tarea de la cuadrícula de verificación en primer plano se detiene con el mensaje `Encountered a critical storage error in volume vol1ID`, debe realizar el procedimiento para recuperar un volumen de almacenamiento fallido. Consulte las instrucciones de recuperación y mantenimiento.

Después de terminar

Si aún tiene dudas sobre la integridad de los datos, vaya a **LDR > verificación > Configuración > Principal** y aumente la tasa de verificación de fondo. La verificación en segundo plano comprueba la corrección de todos los datos de objeto almacenados y repara cualquier problema que encuentre. Encontrar y reparar posibles problemas lo más rápidamente posible reduce el riesgo de pérdida de datos.

Información relacionada

["Mantener recuperar"](#)

Solución de problemas de datos de objetos perdidos o faltantes

Los objetos se pueden recuperar por varios motivos, incluidas las solicitudes de lectura de una aplicación cliente, las verificaciones en segundo plano de los datos de objetos replicados, las reevaluaciones de ILM y la restauración de los datos de objetos durante la recuperación de un nodo de almacenamiento.

El sistema StorageGRID utiliza la información de ubicación en los metadatos de un objeto para determinar desde qué ubicación se debe recuperar el objeto. Si no se encuentra una copia del objeto en la ubicación esperada, el sistema intenta recuperar otra copia del objeto desde cualquier otra parte del sistema, suponiendo que la política de ILM contenga una regla para realizar dos o más copias del objeto.

Si esta recuperación se realiza correctamente, el sistema StorageGRID sustituye a la copia del objeto que falta. De lo contrario, se activan la alerta **objetos perdidos** y la alarma legado PERDIDO (objetos perdidos), como se indica a continuación:

- En el caso de las copias replicadas, si no se puede recuperar otra copia, el objeto se considera perdido y se activan alertas y alarmas.

- En el caso de copias codificadas de borrado, si no se puede recuperar una copia de la ubicación esperada, el atributo copias dañadas detectadas (ECOR) aumenta uno antes de intentar recuperar una copia de otra ubicación. Si no se encuentra ninguna otra copia, se activan la alerta y la alarma.

Debe investigar todas las alertas de **objetos perdidos** inmediatamente para determinar la causa raíz de la pérdida y determinar si el objeto puede seguir existiendo sin conexión o, de lo contrario, no disponible actualmente, nodo de almacenamiento o nodo de archivado.

En caso de que se pierdan los datos de objeto sin copias, no existe una solución de recuperación. Sin embargo, debe restablecer el contador objetos perdidos para evitar que objetos perdidos conocidos oculte cualquier objeto perdido nuevo.

Información relacionada

["Investigar objetos perdidos"](#)

["Restablecer el número de objetos perdidos y faltantes"](#)

Investigar objetos perdidos

Cuando se activan la alerta **objetos perdidos** y la alarma legado PERDIDO (objetos perdidos), debe investigar inmediatamente. Recopile información sobre los objetos afectados y póngase en contacto con el soporte técnico.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.
- Debe tener la `Passwords.txt` archivo.

Acerca de esta tarea

La alerta * objetos perdidos* y la alarma PERDIDA indican que StorageGRID cree que no hay copias de un objeto en la cuadrícula. Es posible que los datos se hayan perdido de forma permanente.

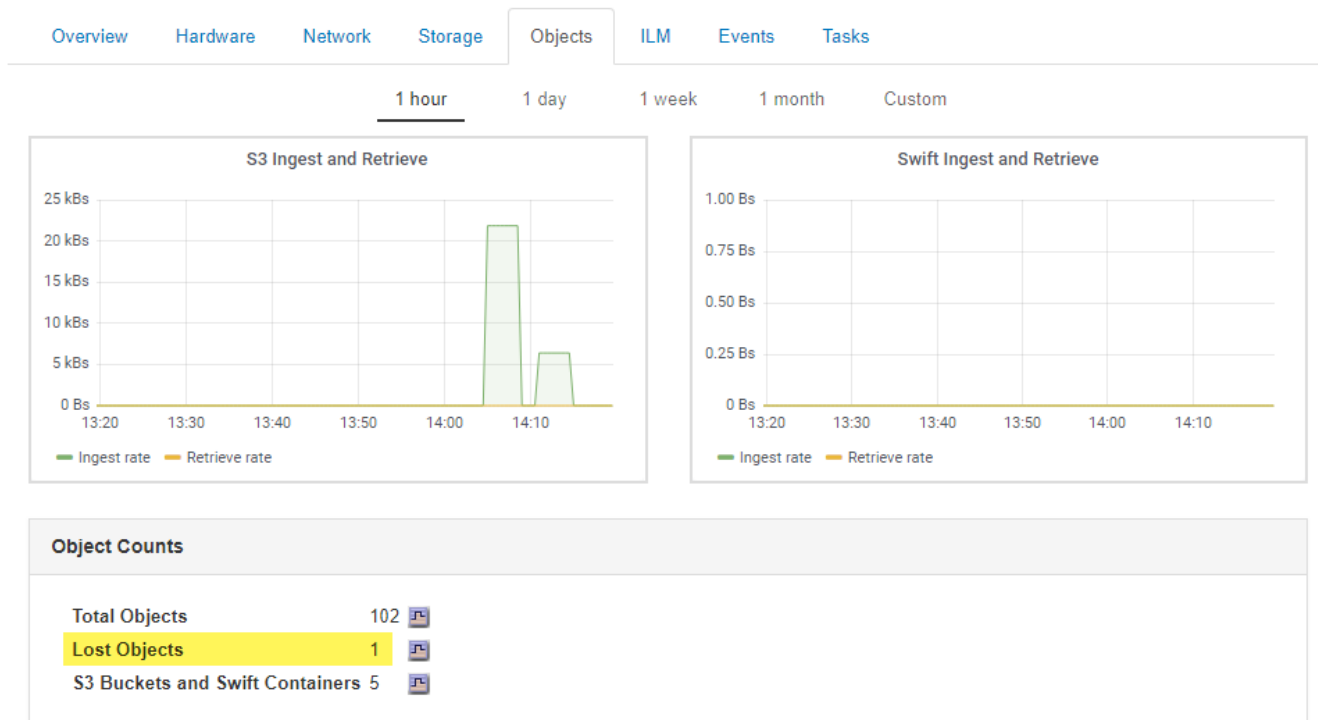
Investigue inmediatamente las alarmas o alertas de objetos perdidos. Es posible que deba tomar medidas para evitar la pérdida de datos adicional. En algunos casos, es posible que pueda restaurar un objeto perdido si realiza una acción rápida.

El número de objetos perdidos se puede ver en el Gestor de grid.

Pasos

1. Seleccione **Nodes**.
2. Seleccione **Storage Node > Objects**.
3. Revise el número de objetos perdidos que se muestra en la tabla recuentos de objetos.

Este número indica el número total de objetos que este nodo de cuadrícula detecta como no recibidos de todo el sistema StorageGRID. El valor es la suma de los contadores de objetos perdidos del componente almacén de datos dentro de los servicios LDR y DDS.



4. Desde un nodo de administración, acceda al registro de auditoría para determinar el identificador único (UUID) del objeto que activó la alerta **objetos perdidos** y la alarma PERDIDA:

a. Inicie sesión en el nodo de grid:

i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`

ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`

iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo. Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

b. Cambie al directorio donde se encuentran los registros de auditoría. Introduzca: `cd /var/local/audit/export/`

c. Utilice `grep` para extraer los mensajes de auditoría de objetos perdidos (OLST). Introduzca: `grep OLST audit_file_name`

d. Observe el valor de UUID incluido en el mensaje.

```
>Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT: [CBID (UI64) :0x38186FE53E3C49A5] [UUID (CSTR) :926026C4-00A4-449B-
AC72-BCCA72DD1311]
[PATH (CSTR) : "source/cats"] [NOID (UI32) :12288733] [VOLI (UI64) :3222345986
] [RSLT (FC32) :NONE] [AVER (UI32) :10]
[ATIM (UI64) :1581535134780426] [ATYP (FC32) :OLST] [ANID (UI32) :12448208] [A
MID (FC32) :ILMX] [ATID (UI64) :7729403978647354233]]
```

5. Utilice la `ObjectByUUID` Comando para encontrar el objeto mediante su identificador (UUID) y, a continuación, determinar si los datos están en riesgo.
 - a. Telnet a localhost 1402 para acceder a la consola LDR.
 - b. Introduzca: `/proc/OBRP/ObjectByUUID UUID_value`

En este primer ejemplo, el objeto con UUID 926026C4-00A4-449B-AC72-BCCA72DD1311 tiene dos ubicaciones en la lista.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
  "TYPE(Object Type)": "Data object",
  "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
  "NAME": "cats",
  "CBID": "0x38186FE53E3C49A5",
  "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
  "PPTH(Parent path)": "source",
  "META": {
    "BASE(Protocol metadata)": {
      "PAWS(S3 protocol version)": "2",
      "ACCT(S3 account ID)": "44084621669730638018",
      "*ctp(HTTP content MIME type)": "binary/octet-stream"
    },
    "BYCB(System metadata)": {
      "CSIZ(Plaintext object size)": "5242880",
      "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
      "BSIZ(Content block size)": "5252084",
      "CVER(Content block version)": "196612",
      "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
      "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
      "ITME": "1581534970983000"
    },
    "CMSM": {
      "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
    },
    "AWS3": {
      "LOCC": "us-east-1"
    }
  },
},
```



```

"CLCO\ (Locations\)": \[
  \{
    "Location Type": "CLDI\ (Location online\)",
    "NOID\ (Node ID\)": "12448208",
    "VOLI\ (Volume ID\)": "3222345473",
    "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
    "LTIM\ (Location timestamp\)": "2020-02-
12T19:36:17.880569"
  },
  \{
    "Location Type": "CLDI\ (Location online\)",
    "NOID\ (Node ID\)": "12288733",
    "VOLI\ (Volume ID\)": "3222345984",
    "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
    "LTIM\ (Location timestamp\)": "2020-02-
12T19:36:17.934425"
  }
]
}

```

En el segundo ejemplo, el objeto con UUID 926026C4-00A4-449B-AC72-BCCA72DD1311 no tiene ninguna ubicación en la lista.

```
ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311
```

```
{
  "TYPE(Object Type)": "Data object",
  "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
  "NAME": "cats",
  "CBID": "0x38186FE53E3C49A5",
  "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
  "PPTH(Parent path)": "source",
  "META": {
    "BASE(Protocol metadata)": {
      "PAWS(S3 protocol version)": "2",
      "ACCT(S3 account ID)": "44084621669730638018",
      "*ctp(HTTP content MIME type)": "binary/octet-stream"
    },
    "BYCB(System metadata)": {
      "CSIZ(Plaintext object size)": "5242880",
      "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
      "BSIZ(Content block size)": "5252084",
      "CVER(Content block version)": "196612",
      "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
      "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
      "ITME": "1581534970983000"
    },
    "CMSM": {
      "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
    },
    "AWS3": {
      "LOCC": "us-east-1"
    }
  }
}
```

a. Revise el resultado de /proc/OBRP/ObjectByUUID y realice la acción correspondiente:

Metadatos	Conclusión
No se ha encontrado ningún objeto ("ERROR": "")	<p>Si no se encuentra el objeto, se devuelve el mensaje "ERROR":".</p> <p>Si no se encuentra el objeto, es seguro ignorar la alarma. La falta de un objeto indica que el objeto se ha eliminado intencionalmente.</p>
Ubicaciones > 0	<p>Si hay ubicaciones enumeradas en la salida, la alarma objetos perdidos puede ser un falso positivo.</p> <p>Confirme que los objetos existen. Utilice el Id. De nodo y la ruta de archivo que aparecen en la salida para confirmar que el archivo de objeto está en la ubicación de la lista.</p> <p>(El procedimiento para buscar objetos potencialmente perdidos explica cómo usar el ID de nodo para encontrar el nodo de almacenamiento correcto).</p> <p>"Buscar y restaurar objetos potencialmente perdidos"</p> <p>Si los objetos existen, puede restablecer el recuento de objetos perdidos para borrar la alarma y la alerta.</p>
Ubicaciones = 0	<p>Si no hay ninguna ubicación en la salida, el objeto puede faltar. Puede intentar encontrar y restaurar el objeto por su cuenta, o bien ponerse en contacto con el soporte técnico.</p> <p>"Buscar y restaurar objetos potencialmente perdidos"</p> <p>Es posible que el soporte técnico le solicite determinar si hay un procedimiento de recuperación del almacenamiento en curso. Es decir, ¿se ha emitido un comando <i>repair-data</i> en cualquier nodo de almacenamiento y la recuperación sigue en curso? Consulte la información sobre cómo restaurar datos de objeto en un volumen de almacenamiento en las instrucciones de recuperación y mantenimiento.</p>

Información relacionada

["Mantener recuperar"](#)

["Revisar los registros de auditoría"](#)

Buscar y restaurar objetos potencialmente perdidos

Puede ser posible encontrar y restaurar objetos que han activado una alarma objetos perdidos (PERDIDOS) y una alerta **objeto perdido** y que se ha identificado como potencialmente perdido.

Lo que necesitará

- Debe tener el UUID de cualquier objeto perdido, tal como se identifica en "investigar objetos perdidos".
- Debe tener la `Passwords.txt` archivo.

Acerca de esta tarea

Puede seguir este procedimiento para buscar copias replicadas del objeto perdido en otra parte de la cuadrícula. En la mayoría de los casos, el objeto perdido no se encuentra. Sin embargo, en algunos casos, es posible que pueda encontrar y restaurar un objeto replicado perdido si realiza una acción rápida.



Póngase en contacto con el soporte técnico para obtener ayuda con este procedimiento.

Pasos

1. En un nodo de administrador, busque los registros de auditoría para las posibles ubicaciones de objetos:

a. Inicie sesión en el nodo de grid:

- i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
- ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
- iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
- iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo. Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

b. Cambie al directorio donde se encuentran los registros de auditoría: `cd /var/local/audit/export/`

c. Utilice `grep` para extraer los mensajes de auditoría asociados con el objeto potencialmente perdido y enviarlos a un archivo de salida. Introduzca: `grep uuid-valueaudit_file_name > output_file_name`

Por ejemplo:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_lost_object.txt
```

d. Utilice `grep` para extraer los mensajes de auditoría de ubicación perdida (LLST) de este archivo de salida. Introduzca: `grep LLST output_file_name`

Por ejemplo:

```
Admin: # grep LLST messages_about_lost_objects.txt
```

Un mensaje de auditoría LLST se parece a este mensaje de ejemplo.

```
[AUDT:\[NOID\ (UI32\):12448208\] [CBIL (UI64) :0x38186FE53E3C49A5]
[UUID (CSTR) : "926026C4-00A4-449B-AC72-BCCA72DD1311"] [LTYP (FC32) :CLDI]
[PCLD\ (CSTR\): "/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
[TSRC (FC32) :SYST] [RSLT (FC32) :NONE] [AVER (UI32) :10] [ATIM (UI64) :
1581535134379225] [ATYP (FC32) :LLST] [ANID (UI32) :12448208] [AMID (FC32) :CL
SM]
[ATID (UI64) :7086871083190743409]]
```

e. Busque el campo PCLD y EL campo NOID en el mensaje LLST.

Si está presente, el valor de PCLD es la ruta completa del disco a la copia del objeto replicado que falta. El valor DE NOID es el ID de nodo de la LDR, donde se puede encontrar una copia del objeto.

Si encuentra una ubicación de objeto, es posible que pueda restaurar el objeto.

f. Busque el nodo de almacenamiento para este ID de nodo LDR.

El ID de nodo se puede usar de dos formas de encontrar el nodo de almacenamiento:

- En Grid Manager, seleccione **Soporte > Herramientas > Topología de cuadrícula**. A continuación, seleccione **Data Center > Storage Node > LDR**. El ID del nodo LDR se encuentra en la tabla Información del nodo. Revise la información de cada nodo de almacenamiento hasta que encuentre el que aloja esta LDR.
- Descargue y descomprima el paquete de recuperación para el grid. Hay un directorio `\docs` en DICHO paquete. Si abre el archivo `index.html`, el Resumen de servidores muestra todos los ID de nodo para todos los nodos de cuadrícula.

2. Determine si el objeto existe en el nodo de almacenamiento que se indica en el mensaje de auditoría:

a. Inicie sesión en el nodo de grid:

- i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
- ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
- iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
- iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo.

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

b. Determine si existe la ruta del archivo para el objeto.

Para la ruta de acceso del archivo del objeto, utilice el valor de PCLD del mensaje de auditoría LLST.

Por ejemplo, introduzca:

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Nota: Siempre encierre la ruta del archivo de objeto entre comillas simples en comandos para escapar de cualquier carácter especial.

- Si no se encuentra la ruta de objeto, se pierde el objeto y no se puede restaurar con este procedimiento. Póngase en contacto con el soporte técnico.
- Si se encuentra la ruta del objeto, continúe con el paso [Restaura el objeto en StorageGRID](#). Puede intentar restaurar el objeto encontrado de nuevo en StorageGRID.

1. Si se encontró la ruta del objeto, intente restaurar el objeto a StorageGRID:

- a. Desde el mismo nodo de almacenamiento, cambie la propiedad del archivo de objetos para que StorageGRID lo pueda gestionar. Introduzca: `chown ldr-user:bycast 'file_path_of_object'`
- b. Telnet a localhost 1402 para acceder a la consola LDR. Introduzca: `telnet 0 1402`

c. Introduzca: `cd /proc/STOR`

d. Introduzca: `Object_Found 'file_path_of_object'`

Por ejemplo, introduzca:

```
Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Emitir el `Object_Found` command notifica a la cuadrícula la ubicación del objeto. También activa la política de ILM activa, con la que se realizan copias adicionales según se especifique en la política.

Nota: Si el nodo de almacenamiento donde encontró el objeto está sin conexión, puede copiar el objeto en cualquier nodo de almacenamiento que esté en línea. Coloque el objeto en cualquier directorio `/var/local/rangedb` del nodo de almacenamiento en línea. A continuación, emita el `Object_Found` comando que usa esa ruta de acceso al objeto.

- Si el objeto no se puede restaurar, el `Object_Found` error del comando. Póngase en contacto con el soporte técnico.
- Si el objeto se restauró correctamente en StorageGRID, aparece un mensaje de éxito. Por ejemplo:

```
ade 12448208: /proc/STOR > Object_Found
'/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

ade 12448208: /proc/STOR > Object found succeeded.
First packet of file was valid. Extracted key: 38186FE53E3C49A5
Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
'/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
```

Continúe con el paso [Compruebe que se han creado nuevas ubicaciones](#)

1. Si el objeto se restauró correctamente en StorageGRID, compruebe que se crearon nuevas ubicaciones.

a. Introduzca: `cd /proc/OBRP`

b. Introduzca: `ObjectByUUID UUID_value`

El ejemplo siguiente muestra que hay dos ubicaciones para el objeto con el UUID 926026C4-00A4-449B-AC72-BCCA72DD1311.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
  "TYPE(Object Type)": "Data object",
  "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
  "NAME": "cats",
```

```

"CBID": "0x38186FE53E3C49A5",
"PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
"PPTH(Parent path)": "source",
"META": {
  "BASE(Protocol metadata)": {
    "PAWS(S3 protocol version)": "2",
    "ACCT(S3 account ID)": "44084621669730638018",
    "*ctp(HTTP content MIME type)": "binary/octet-stream"
  },
  "BYCB(System metadata)": {
    "CSIZ(Plaintext object size)": "5242880",
    "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
    "BSIZ(Content block size)": "5252084",
    "CVER(Content block version)": "196612",
    "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
    "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
    "ITME": "1581534970983000"
  },
  "CMSM": {
    "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
  },
  "AWS3": {
    "LOCC": "us-east-1"
  }
},
"CLCO\ (Locations\)": \[
  \{
    "Location Type": "CLDI\ (Location online\)",
    "NOID\ (Node ID\)": "12448208",
    "VOLLI\ (Volume ID\)": "3222345473",
    "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
    "LTIM\ (Location timestamp\)": "2020-02-12T19:36:17.880569"
  },
  \{
    "Location Type": "CLDI\ (Location online\)",
    "NOID\ (Node ID\)": "12288733",
    "VOLLI\ (Volume ID\)": "3222345984",
    "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
    "LTIM\ (Location timestamp\)": "2020-02-12T19:36:17.934425"
  }
}

```

```
]
}
```

- a. Cierre la sesión en la consola LDR. Introduzca: `exit`
2. En un nodo de administración, busque en los registros de auditoría del mensaje de auditoría ORLM de este objeto para confirmar que la gestión del ciclo de vida de la información (ILM) ha colocado las copias según sea necesario.

- a. Inicie sesión en el nodo de grid:

- i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
- ii. Introduzca la contraseña que aparece en `Passwords.txt` archivo.
- iii. Introduzca el siguiente comando para cambiar a la raíz: `su -`
- iv. Introduzca la contraseña que aparece en `Passwords.txt` archivo. Cuando ha iniciado sesión como root, el símbolo del sistema cambia de `$` para `#`.

- b. Cambie al directorio donde se encuentran los registros de auditoría: `cd /var/local/audit/export/`

- c. Utilice `grep` para extraer los mensajes de auditoría asociados con el objeto en un archivo de salida. Introduzca: `grep uuid-valueaudit_file_name > output_file_name`

Por ejemplo:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_restored_object.txt
```

- d. Utilice `grep` para extraer los mensajes de auditoría Object Rules MET (ORLM) de este archivo de salida. Introduzca: `grep ORLM output_file_name`

Por ejemplo:

```
Admin: # grep ORLM messages_about_restored_object.txt
```

Un mensaje de auditoría ORLM se parece a este mensaje de ejemplo.

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

- a. Busque el campo `LOCS` en el mensaje de auditoría.

Si está presente, el valor de CLDI en LOCS es el ID de nodo y el ID de volumen donde se ha creado una copia de objeto. Este mensaje muestra que se ha aplicado el ILM y que se han creado dos copias de objetos en dos ubicaciones de la cuadrícula.

b. Restablezca el recuento de objetos perdidos en el Gestor de grid.

Información relacionada

["Investigar objetos perdidos"](#)

["Confirmación de ubicaciones de datos de objeto"](#)

["Restablecer el número de objetos perdidos y faltantes"](#)

["Revisar los registros de auditoría"](#)

Restablecer el número de objetos perdidos y faltantes

Después de investigar el sistema StorageGRID y comprobar que todos los objetos perdidos registrados se pierden permanentemente o que se trata de una alarma falsa, puede restablecer el valor del atributo objetos perdidos a cero.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

Puede restablecer el contador objetos perdidos desde cualquiera de las siguientes páginas:

- **Soporte > Herramientas > Topología de cuadrícula > *site* > *nodo de almacenamiento* > LDR > almacén de datos > Descripción general > Principal**
- **Soporte > Herramientas > Topología de cuadrícula > *site* > *nodo de almacenamiento* > DDS > almacén de datos > Descripción general > Principal**


Estas instrucciones muestran cómo reiniciar el contador desde la página **LDR > Data Store**.

Pasos

1. Seleccione **Soporte > Herramientas > Topología de cuadrícula**.
2. Seleccione **Site > Storage Node > LDR > Data Store > Configuración** para el nodo de almacenamiento que tiene la alerta **objetos perdidos** o la alarma PERDIDA.
3. Seleccione **Restablecer recuento de objetos perdidos**.

Overview | Alarms | Reports | **Configuration**

Main | Alarms

 **Configuration: LDR (99-94) - Data Store**
 Updated: 2017-05-11 14:56:13 PDT

Reset Lost Objects Count

Apply Changes 

4. Haga clic en **aplicar cambios**.

El atributo objetos perdidos se restablece a 0 y la alerta **objetos perdidos** y la alarma PERDIDA se borra, lo que puede tardar unos minutos.

5. De forma opcional, restablezca otros valores de atributos relacionados que pueden haberse incrementado en el proceso de identificación del objeto perdido.

- a. Seleccione **Site > Storage Node > LDR > código de borrado > Configuración**.
- b. Seleccione **Restablecer errores de lectura recuento** y **Restablecer copias corruptas número detectado**.
- c. Haga clic en **aplicar cambios**.
- d. Seleccione **Site > Storage Node > LDR > Verification > Configuration**.
- e. Seleccione **Restablecer recuento de objetos ausentes** y **Restablecer recuento de objetos corruptos**.
- f. Si está seguro de que los objetos en cuarentena no son necesarios, puede seleccionar **Eliminar objetos en cuarentena**.

Los objetos en cuarentena se crean cuando la verificación en segundo plano identifica una copia de objeto replicada dañada. En la mayoría de los casos StorageGRID sustituye automáticamente el objeto dañado y es seguro eliminar los objetos en cuarentena. Sin embargo, si se activa la alerta **objetos perdidos** o la alarma PERDIDA, es posible que el soporte técnico desee acceder a los objetos en cuarentena.

g. Haga clic en **aplicar cambios**.

Puede tardar unos momentos en que los atributos se restablezcan después de hacer clic en **aplicar cambios**.

Información relacionada

["Administre StorageGRID"](#)

Solución de problemas de la alerta de almacenamiento de datos de objeto Low

La alerta **almacenamiento de objetos bajo** supervisa cuánto espacio está disponible para almacenar datos de objetos en cada nodo de almacenamiento.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

El **almacenamiento de datos de objetos bajo** se activa cuando la cantidad total de datos de objetos codificados replicados y de borrado en un nodo de almacenamiento cumple una de las condiciones configuradas en la regla de alerta.

De forma predeterminada, se activa una alerta principal cuando esta condición se evalúa como TRUE:

```
(storagegrid_storage_utilization_data_bytes/  
(storagegrid_storage_utilization_data_bytes +  
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

En esta condición:

- `storagegrid_storage_utilization_data_bytes` Es una estimación del tamaño total de los datos de objetos codificados de replicación y borrado para un nodo de almacenamiento.
- `storagegrid_storage_utilization_usable_space_bytes` Es la cantidad total de espacio de almacenamiento de objetos que queda para un nodo de almacenamiento.

Si se activa una alerta de **almacenamiento de datos de objeto bajo** importante o menor, debe realizar un procedimiento de expansión Lo antes posible..

Pasos

1. Seleccione **Alertas > corriente**.

Aparece la página Alertas.

2. En la tabla de alertas, expanda el grupo de alertas **almacenamiento de datos de objeto bajo**, si es necesario, y seleccione la alerta que desea ver.



Seleccione la alerta, no el encabezado de un grupo de alertas.

3. Revise los detalles en el cuadro de diálogo y tenga en cuenta lo siguiente:

- Tiempo activado
- El nombre del sitio y del nodo
- Los valores actuales de las métricas de esta alerta

4. Seleccione **Nodes > Storage Node o Site > Storage**.

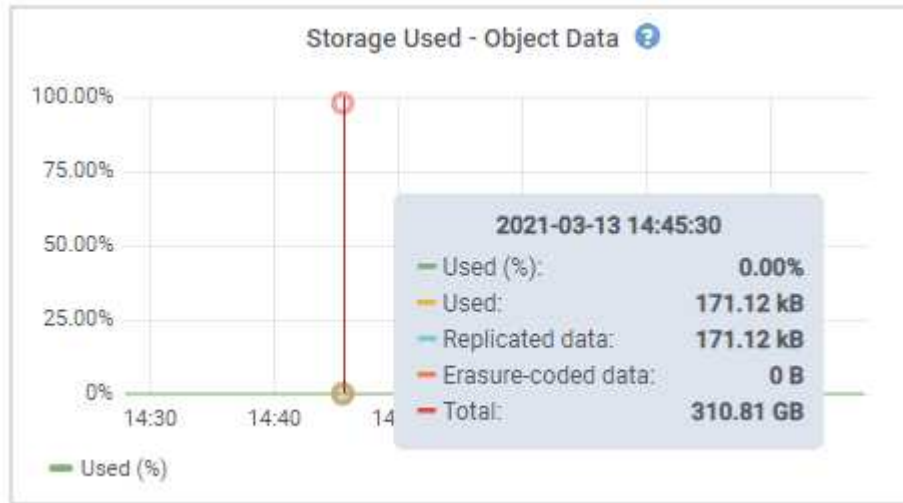
5. Pase el cursor sobre el gráfico almacenamiento utilizado - datos de objeto.

Se muestran los siguientes valores:

- **Usado (%)**: El porcentaje del espacio útil total que se ha utilizado para datos de objeto.
- **Utilizado**: La cantidad de espacio útil total que se ha utilizado para los datos de objeto.
- **Datos replicados**: Estimación de la cantidad de datos de objetos replicados en este nodo, sitio o

cuadrícula.

- **Datos codificados por borrado:** Estimación de la cantidad de datos de objetos codificados por borrado en este nodo, sitio o cuadrícula.
- **Total:** La cantidad total de espacio utilizable en este nodo, sitio o cuadrícula. El valor utilizado es `storagegrid_storage_utilization_data_bytes` métrico.



6. Seleccione los controles de tiempo encima del gráfico para ver el uso del almacenamiento en diferentes periodos de tiempo.

Si se mira el uso del almacenamiento a lo largo del tiempo, puede comprender cuánto almacenamiento se utilizó antes y después de que se activó la alerta, y puede ayudar a calcular cuánto tiempo podría tardar en llenarse el espacio restante del nodo.

7. Lo antes posible., realice un procedimiento de ampliación para añadir capacidad de almacenamiento.

Es posible añadir volúmenes de almacenamiento (LUN) a los nodos de almacenamiento existentes, o bien añadir nuevos nodos de almacenamiento.



Para gestionar un nodo de almacenamiento completo, consulte las instrucciones para administrar StorageGRID.

Información relacionada

["Solución de problemas de la alarma de estado de almacenamiento \(SST\)"](#)

["Amplíe su grid"](#)

["Administre StorageGRID"](#)

Solución de problemas de la alarma de estado de almacenamiento (SST)

La alarma de estado del almacenamiento (SST) se activa si un nodo de almacenamiento no tiene suficiente espacio libre restante para el almacenamiento de objetos.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

La alarma SSTS (Estado de almacenamiento) se activa en el nivel de aviso cuando la cantidad de espacio libre en cada volumen de un nodo de almacenamiento cae por debajo del valor de la Marca de agua de sólo lectura suave del volumen de almacenamiento (**Configuración > Opciones de almacenamiento > Descripción general**).



Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

Por ejemplo, supongamos que la Marca de agua de sólo lectura suave del volumen de almacenamiento se establece en 10 GB, que es su valor predeterminado. La alarma SSTS se activa si queda menos de 10 GB de espacio utilizable en cada volumen de almacenamiento del nodo de almacenamiento. Si alguno de los volúmenes tiene 10 GB o más de espacio disponible, la alarma no se activa.

Si se ha activado una alarma SSTS, puede seguir estos pasos para comprender mejor el problema.

Pasos

1. Seleccione **Soporte > Alarmas (heredadas) > Alarmas actuales**.
2. En la columna Servicio, seleccione el centro de datos, el nodo y el servicio asociados a la alarma SSTS.

Aparece la página Topología de cuadrícula. La ficha Alarmas muestra las alarmas activas del nodo y el servicio que ha seleccionado.



Alarms: LDR (DC1-S3-101-195) - Storage

Updated: 2019-10-09 12:52:43 MDT

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Notice	SSTS (Storage Status)	Insufficient Free Space	2019-10-09 12:42:51 MDT	Insufficient Free Space	Insufficient Free Space		<input type="checkbox"/>
Notice	SAVP (Total Usable Space (Percent))	Under 10 %	2019-10-09 12:43:21 MDT	7.95 %	7.95 %		<input type="checkbox"/>
Normal	SHLH (Health)						<input type="checkbox"/>

Apply Changes

En este ejemplo, se han activado las alarmas SSTS (Estado del almacenamiento) y SAVP (espacio útil total (porcentaje)) en el nivel de aviso.







Normalmente, tanto LA alarma SSTS como la alarma SAVP se activan aproximadamente al mismo tiempo; sin embargo, si ambas alarmas se activan depende del valor de la Marca de agua en GB y del valor de la alarma SAVP en porcentaje.

- Para determinar cuánto espacio útil está realmente disponible, seleccione **LDR > almacenamiento > Descripción general** y busque el atributo espacio útil total (STS).







Overview Alarms Reports Configuration

Main







 Overview: LDR (:DC1-S1-101-193) - Storage
Updated: 2019-10-09 12:51:07 MDT

Storage State - Desired:	Online	
Storage State - Current:	Read-only	
Storage Status:	Insufficient Free Space	 
















Utilization

Total Space:	164 GB	
Total Usable Space:	19.6 GB	
Total Usable Space (Percent):	11.937 %	 
Total Data:	139 GB	
Total Data (Percent):	84.567 %	

Replication

Block Reads:	0	
Block Writes:	2,279,881	
Objects Retrieved:	0	
Objects Committed:	88,882	
Objects Deleted:	16	
Delete Service State:	Enabled	

Object Store Volumes

ID	Total	Available	Replicated Data	EC Data	Stored (%)	Health
0000	54.7 GB	2.93 GB	 46.2 GB	 0 B	 84.486 %	No Errors  
0001	54.7 GB	8.32 GB	 46.3 GB	 0 B	 84.644 %	No Errors  
0002	54.7 GB	8.36 GB	 46.3 GB	 0 B	 84.57 %	No Errors  

En este ejemplo, solo quedan disponibles 19.6 GB del espacio de 164 GB en este nodo de almacenamiento. Tenga en cuenta que el valor total es la suma de los valores **disponible** para los tres volúmenes de almacén de objetos. Se activó la alarma DE SSTS porque cada uno de los tres volúmenes de almacenamiento tenía menos de 10 GB de espacio disponible.

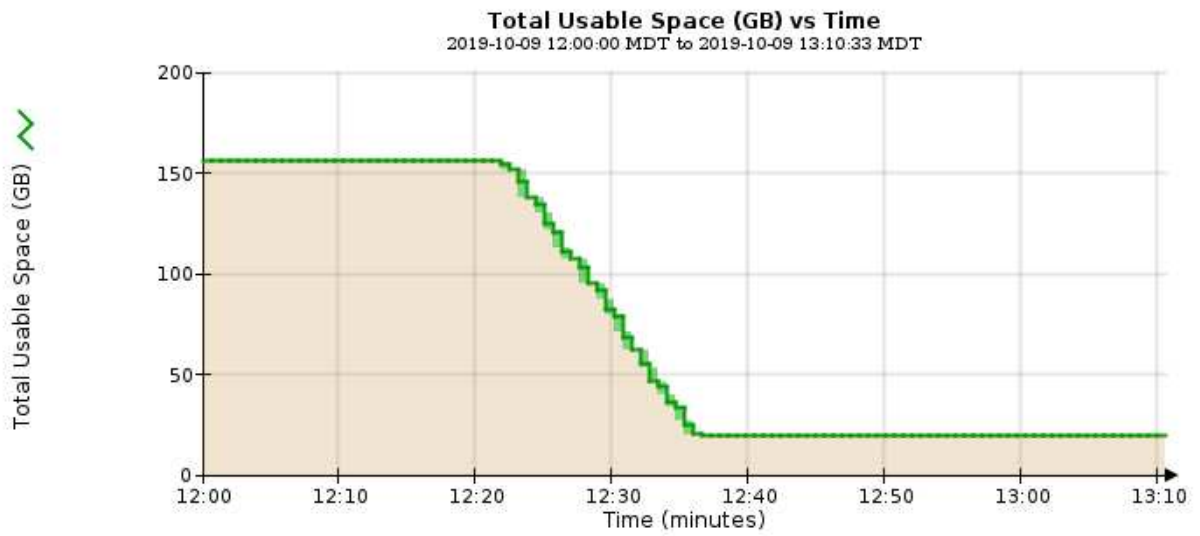
- Para comprender cómo se ha utilizado el almacenamiento a lo largo del tiempo, seleccione la ficha **Informes** y Trace el espacio útil total en las últimas horas.

En este ejemplo, el espacio útil total cayó de aproximadamente 155 GB a 12:00 a 20 GB a 12:35, lo que corresponde al tiempo en que se activó la alarma DE SST.



Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute:	Total Usable Space	Vertical Scaling:	<input checked="" type="checkbox"/>	Start Date:	2019/10/09 12:00:00
Quick Query:	Custom Query	Raw Data:	<input type="checkbox"/>	End Date:	2019/10/09 13:10:33




- Para entender cómo se utiliza el almacenamiento como un porcentaje del total, graficar espacio útil total (porcentaje) durante las últimas horas.

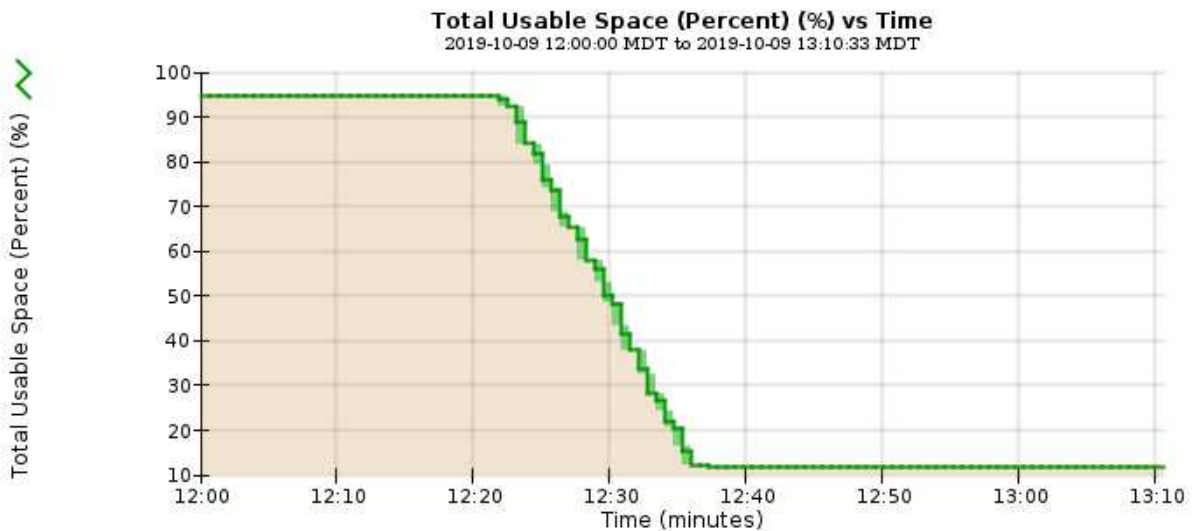
En este ejemplo, el espacio total utilizable cayó de un 95% a algo más de un 10% aproximadamente al mismo tiempo.

Overview | Alarms | **Reports** | Configuration

Charts | Text

 Reports (Charts): LDR (DC1-S1-101-193) - Storage

Attribute: Total Usable Space (Percent) Vertical Scaling: Start Date: 2019/10/09 12:00:00
 Quick Query: Custom Query Update Raw Data: End Date: 2019/10/09 13:10:33



6. Según sea necesario, amplíe el sistema StorageGRID para ampliar la capacidad de almacenamiento.

Para obtener procedimientos sobre cómo gestionar un nodo de almacenamiento completo, consulte las instrucciones para administrar StorageGRID.

Información relacionada

["Amplíe su grid"](#)

["Administre StorageGRID"](#)

Solución de problemas de la entrega de mensajes de servicios de la plataforma (alarma SMTT)

La alarma total de eventos (SMTT) se activa en Grid Manager si se envía un mensaje de servicio de plataforma a un destino que no puede aceptar los datos.

Acerca de esta tarea

Por ejemplo, la carga de varias partes de S3 puede realizarse correctamente aunque no se pueda enviar el mensaje de notificación o replicación asociado al extremo configurado. O bien, puede no producirse un error en el mensaje de la replicación de CloudMirror si los metadatos son demasiado largos.

La alarma SMTT contiene un mensaje de último evento que dice: `Failed to publish notifications for bucket-name object key` para el último objeto cuya notificación falló.

Para obtener información adicional sobre la solución de problemas de los servicios de la plataforma, consulte las instrucciones para administrar StorageGRID. Es posible que necesite acceder al inquilino desde el Administrador de inquilinos para depurar un error de servicio de plataforma.

Pasos

1. Para ver la alarma, seleccione **Nodes > site > grid node > Events**.
2. Ver último evento en la parte superior de la tabla.

Los mensajes de eventos también se muestran en la `/var/local/log/bycast-err.log`.

3. Siga las instrucciones proporcionadas en el contenido de la alarma SMTT para corregir el problema.
4. Haga clic en **Restablecer recuentos de eventos**.
5. Notifique al inquilino los objetos cuyos mensajes de servicios de plataforma no se han entregado.
6. Indique al inquilino que active la replicación o notificación fallida actualizando los metadatos o las etiquetas del objeto.

Información relacionada

["Administre StorageGRID"](#)

["Usar una cuenta de inquilino"](#)

["Referencia de archivos de registro"](#)

["Restableciendo el número de eventos"](#)

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.