



Solucionar los problemas de un sistema StorageGRID

StorageGRID 11.5

NetApp
April 11, 2024

Tabla de contenidos

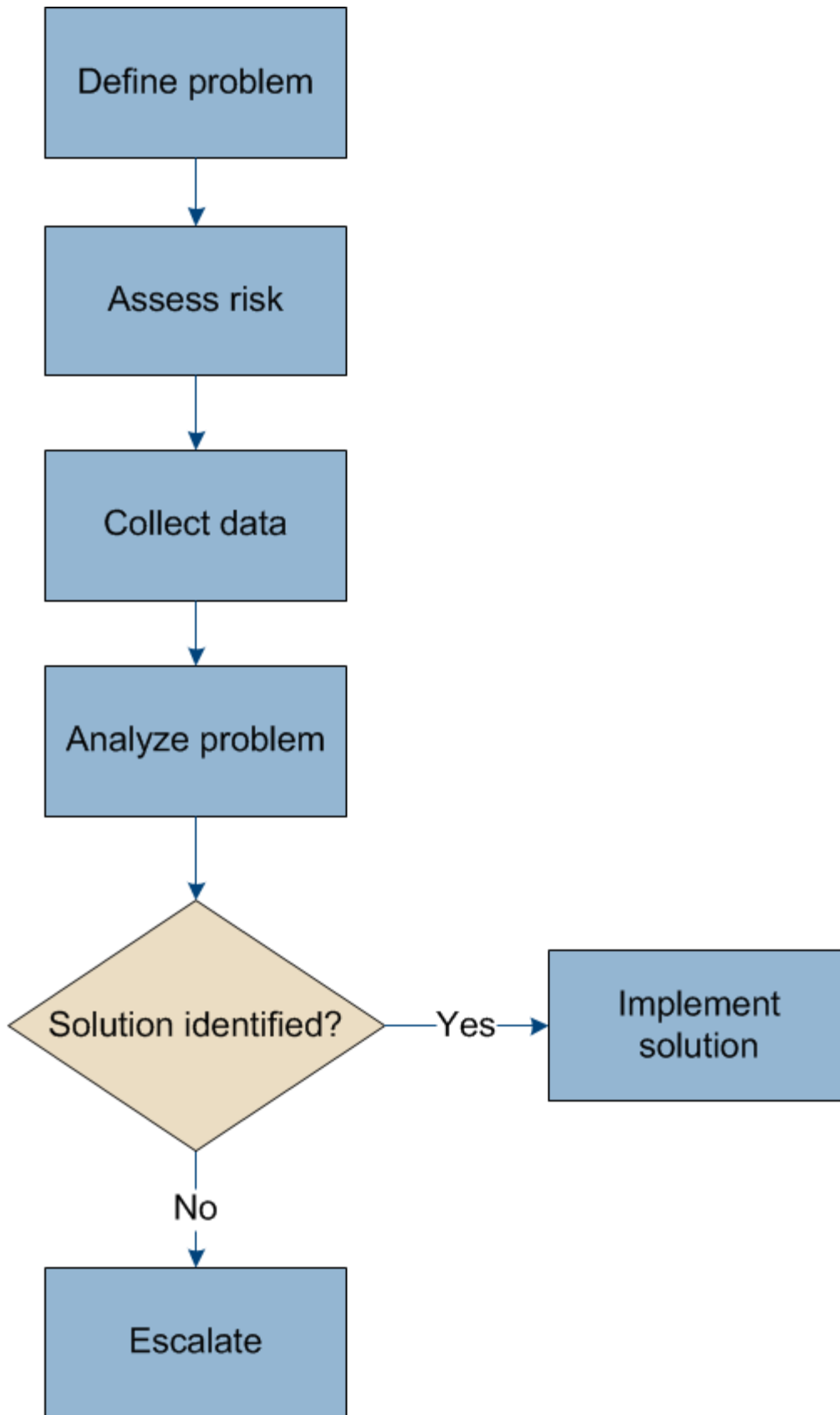
- Solucionar los problemas de un sistema StorageGRID 1
 - Descripción general de la determinación de problemas 1
 - Solucionar problemas de objetos y almacenamiento 9
 - Resolución de problemas de metadatos 41
 - Solución de errores de certificado 48
 - Solucionar problemas del nodo de administrador y de la interfaz de usuario 50
 - Resolución de problemas de red, hardware y plataforma 55

Solucionar los problemas de un sistema StorageGRID

Si tiene algún problema al usar un sistema StorageGRID, consulte las sugerencias y directrices de esta sección para obtener ayuda a la hora de determinar y resolver el problema.

Descripción general de la determinación de problemas

Si se produce un problema al administrar un sistema StorageGRID, puede usar el proceso descrito en esta figura para identificar y analizar el problema. En muchos casos, es posible que pueda resolver problemas por su cuenta; sin embargo, es posible que deba derivar algunos problemas al soporte técnico.



Definición del problema

El primer paso para resolver un problema es definir el problema claramente.

En esta tabla, se proporcionan ejemplos de los tipos de información que pueden recopilar para definir un problema:

Pregunta	Ejemplo de respuesta
¿Qué está haciendo o no el sistema StorageGRID? ¿Cuáles son sus síntomas?	Las aplicaciones cliente informan de que los objetos no se pueden procesar en StorageGRID.
¿Cuándo comenzó el problema?	La ingesta de objetos fue denegada por primera vez a las 14:50 del 8 de enero de 2020.
¿Cómo notó el problema por primera vez?	Notificado por la aplicación cliente. También ha recibido notificaciones por correo electrónico de alerta.
¿El problema ocurre de manera consistente, o sólo a veces?	El problema está en curso.
Si el problema ocurre con regularidad, ¿qué pasos hacen que ocurra	El problema se produce cada vez que un cliente intenta procesar un objeto.
Si el problema ocurre intermitentemente, ¿cuándo ocurre? Registre las horas de cada incidente que conozca.	El problema no es intermitente.
¿Ha visto este problema con anterioridad? ¿Con qué frecuencia ha tenido este problema en el pasado?	Esta es la primera vez que veo este asunto.

Evaluación del riesgo y del impacto en el sistema

Una vez que haya definido el problema, evalúe su riesgo y su impacto en el sistema StorageGRID. Por ejemplo, la presencia de alertas cruciales no necesariamente significa que el sistema no esté proporcionando servicios básicos.

En esta tabla se resume el impacto que tiene el problema de ejemplo en las operaciones del sistema:

Pregunta	Ejemplo de respuesta
¿El sistema StorageGRID puede procesar contenido?	No
¿Las aplicaciones cliente pueden recuperar contenido?	Algunos objetos se pueden recuperar y otros no.
¿Los datos están en riesgo?	No
¿Se ve gravemente afectada la capacidad para llevar a cabo operaciones empresariales?	Sí, porque las aplicaciones cliente no pueden almacenar objetos en el sistema StorageGRID y los datos no pueden recuperarse de forma coherente.

Recogida de datos

Una vez definido el problema y haya evaluado su riesgo e impacto, recopile los datos para su análisis. El tipo de datos más útiles para recopilar depende de la naturaleza del problema.

Tipo de datos que se van a recoger	Por qué recoger estos datos	Instrucciones
Crear una línea de tiempo de los cambios recientes	Los cambios realizados en el sistema StorageGRID, su configuración o su entorno pueden provocar nuevos comportamientos.	<ul style="list-style-type: none"> • Crear una línea de tiempo de cambios recientes
Revise las alertas y alarmas	<p>Las alertas y alarmas pueden ayudarle a determinar rápidamente la causa raíz de un problema, proporcionando pistas importantes sobre los problemas subyacentes que podrían estar causando.</p> <p>Revise la lista de alertas y alarmas actuales para ver si StorageGRID ha identificado la causa raíz de un problema.</p> <p>Revise las alertas y alarmas activadas en el pasado para obtener información adicional.</p>	<ul style="list-style-type: none"> • "Ver las alertas actuales" • "Visualización de alarmas heredadas" • "Ver alertas resueltas" • "Revisión de las alarmas históricas y la frecuencia de las alarmas (sistema heredado)"
Supervisar eventos	Entre los eventos se incluye cualquier evento de error del sistema o fallo de un nodo, incluidos errores como errores de red. Supervisar eventos para obtener más información acerca de problemas o para ayudar en la solución de problemas.	<ul style="list-style-type: none"> • "Ver la pestaña Eventos" • "Supervisar eventos"
Identificar tendencias mediante informes de texto y gráficos	Las tendencias pueden proporcionar pistas valiosas acerca de cuándo aparecieron los problemas por primera vez, y pueden ayudarle a entender la rapidez con la que las cosas están cambiando.	<ul style="list-style-type: none"> • "Uso de gráficos e informes"
Establecer líneas base	Recopilar información acerca de los niveles normales de varios valores operativos. Estos valores de referencia y las desviaciones de estas líneas de base pueden proporcionar pistas valiosas.	<ul style="list-style-type: none"> • Establecimiento de líneas base
Realice pruebas de procesamiento y recuperación	Para solucionar problemas de rendimiento con la ingesta y la recuperación, utilice una estación de trabajo para almacenar y recuperar objetos. Compare los resultados con los que se ven al usar la aplicación cliente.	<ul style="list-style-type: none"> • "DE PUT y GET rendimiento"
Revisar los mensajes de auditoría	Revise los mensajes de auditoría para seguir las operaciones de StorageGRID con detalle. Los detalles de los mensajes de auditoría pueden ser útiles para solucionar muchos tipos de problemas, incluidos problemas de rendimiento.	<ul style="list-style-type: none"> • "Revisión de mensajes de auditoría"

Tipo de datos que se van a recoger	Por qué recoger estos datos	Instrucciones
Comprobar la ubicación de objetos y la integridad del almacenamiento	Si tiene problemas de almacenamiento, compruebe que los objetos se encuentren en la ubicación que espera. Compruebe la integridad de los datos de objetos en un nodo de almacenamiento.	"Supervisar las operaciones de verificación de objetos".
Recopile datos para el soporte técnico	Es posible que el soporte técnico le solicite recopilar datos o revisar información específica para ayudar a resolver problemas.	<ul style="list-style-type: none"> • "Recogida de archivos de registro y datos del sistema" • "Activación manual de un mensaje de AutoSupport" • "Revisión de las métricas de soporte"

Crear una línea de tiempo de cambios recientes

Cuando se produce un problema, debe considerar qué ha cambiado recientemente y cuándo se produjeron esos cambios.

- Los cambios realizados en el sistema StorageGRID, su configuración o su entorno pueden provocar nuevos comportamientos.
- Una línea de tiempo de los cambios puede ayudarle a identificar qué cambios podrían ser responsables de un problema y cómo cada cambio podría haber afectado su desarrollo.

Crear una tabla de cambios recientes en el sistema que incluya información acerca de cuándo se produjo cada cambio y cualquier información relevante acerca del cambio, tal información acerca de qué más estaba ocurriendo mientras el cambio estaba en curso:

Momento del cambio	Tipo de cambio	Detalles
Por ejemplo: <ul style="list-style-type: none"> • ¿Cuándo inició la recuperación del nodo? • ¿Cuándo se completó la actualización de software? • ¿Interrumpió el proceso? 	¿Qué ha sucedido? ¿Qué has hecho?	Documente los detalles relevantes sobre el cambio. Por ejemplo: <ul style="list-style-type: none"> • Detalles de los cambios de red. • Qué revisión se instaló. • Cambio de las cargas de trabajo de los clientes. Asegúrese de anotar si se estaba produciendo más de un cambio al mismo tiempo. Por ejemplo, ¿se ha realizado este cambio mientras se estaba realizando una actualización?

Ejemplos de cambios recientes significativos

A continuación se muestran algunos ejemplos de cambios potencialmente importantes:

- ¿El sistema StorageGRID se ha instalado, ampliado o recuperado recientemente?
- ¿Se ha actualizado el sistema recientemente? ¿Se ha aplicado una revisión?
- ¿Se ha reparado o modificado recientemente algún hardware?
- ¿Se ha actualizado la política de ILM?
- ¿Ha cambiado la carga de trabajo del cliente?
- ¿Ha cambiado la aplicación cliente o su comportamiento?
- ¿Ha cambiado los equilibradores de carga, o ha agregado o eliminado un grupo de alta disponibilidad de nodos de administrador o nodos de puerta de enlace?
- ¿Se ha iniciado alguna tarea que puede tardar mucho tiempo en completarse? Entre los ejemplos se incluyen:
 - Recuperación de un nodo de almacenamiento con fallos
 - Decomisionado del nodo de almacenamiento
- ¿Se han realizado cambios en la autenticación de usuario, por ejemplo, añadir un inquilino o cambiar la configuración de LDAP?
- ¿Se está realizando la migración de datos?
- ¿Se han activado o cambiado los servicios de la plataforma recientemente?
- ¿Se ha activado el cumplimiento de normativas recientemente?
- ¿Se han añadido o eliminado pools de almacenamiento en cloud?
- ¿Se han realizado cambios en la compresión o el cifrado del almacenamiento?
- ¿Se han producido cambios en la infraestructura de red? Por ejemplo, VLAN, enrutadores o DNS.
- ¿Se han realizado cambios en los orígenes de NTP?
- ¿Se han realizado cambios en las interfaces de red de cliente, administrador o grid?
- ¿Se ha realizado algún cambio de configuración en el nodo de archivado?
- ¿Se han realizado otros cambios en el sistema StorageGRID o en su entorno?

Establecimiento de líneas base

Puede establecer líneas base para el sistema registrando los niveles normales de varios valores operativos. En el futuro, puede comparar los valores actuales con estas líneas de base para ayudar a detectar y resolver valores anómalos.

Propiedad	Valor	Cómo obtener
Consumo medio de almacenamiento	GB consumidos/día Porcentaje consumido/día	Vaya a Grid Manager. En la página Nodes, seleccione la cuadrícula completa o un sitio y vaya a la pestaña Storage. En el gráfico almacenamiento usado - datos de objeto, busque un punto en el que la línea sea bastante estable. Pase el cursor sobre el gráfico para calcular cuánto almacenamiento consume cada día Puede recopilar esta información para todo el sistema o para un centro de datos específico.

Propiedad	Valor	Cómo obtener
Consumo medio de metadatos	GB consumidos/día Porcentaje consumido/día	<p>Vaya a Grid Manager. En la página Nodes, seleccione la cuadrícula completa o un sitio y vaya a la pestaña Storage.</p> <p>En el gráfico almacenamiento usado - metadatos de objeto, busque un punto en el que la línea sea bastante estable. Pase el cursor sobre el gráfico para calcular cuánto almacenamiento de metadatos se consume cada día</p> <p>Puede recopilar esta información para todo el sistema o para un centro de datos específico.</p>
Tasa de operaciones de S3/Swift	Operaciones por segundo	<p>Vaya a Panel en Grid Manager. En la sección Protocol Operations, consulte los valores para la tasa de S3 y la tasa de Swift.</p> <p>Para ver las tasas y recuentos de procesamiento y recuperación de un sitio o nodo específico, seleccione Nodes > site o Storage Node > objetos. Pase el cursor sobre el gráfico ingesta y recuperación de S3 o Swift.</p>
Han fallado las operaciones de S3/Swift	Operaciones	<p>Seleccione Soporte > Herramientas > Topología de cuadrícula. En la pestaña Overview de la sección API Operations, vea el valor de las operaciones de S3 - Failed o Swift - Failed.</p>
Tasa de evaluación de ILM	Objetos por segundo	<p>En la página Nodes, seleccione grid > ILM.</p> <p>En el gráfico de la cola de ILM, busque un período donde la línea sea bastante estable. Pase el cursor sobre el gráfico para calcular un valor de línea de base para tasa de evaluación para su sistema.</p>
Tasa de análisis de ILM	Objetos por segundo	<p>Seleccione Nodes > grid > ILM.</p> <p>En el gráfico de la cola de ILM, busque un período donde la línea sea bastante estable. Pase el cursor sobre el gráfico para calcular un valor de línea de base para tasa de exploración para su sistema.</p>
Objetos en cola de operaciones del cliente	Objetos por segundo	<p>Seleccione Nodes > grid > ILM.</p> <p>En el gráfico de la cola de ILM, busque un período donde la línea sea bastante estable. Pase el cursor por encima del gráfico para calcular un valor de línea de base para objetos en cola (desde operaciones de cliente) para su sistema.</p>
Latencia media de consultas	Milisegundos	<p>Seleccione Nodes > Storage Node > Objects. En la tabla consultas, vea el valor de latencia media.</p>

Analizando datos


Utilice la información que recopila para determinar la causa del problema y las soluciones potenciales.

El análisis depende-problema, pero en general:

- Localizar puntos de fallo y cuellos de botella mediante las alarmas.
- Reconstruya el historial de problemas con el historial de alarmas y los gráficos.
- Utilice gráficos para buscar anomalías y comparar la situación del problema con el funcionamiento normal.

Lista de comprobación de información de escalado

Si no puede resolver el problema por su cuenta, póngase en contacto con el soporte técnico. Antes de ponerse en contacto con el soporte técnico, recopile la información incluida en la siguiente tabla para facilitar la resolución del problema.

 Elemento	Notas
Declaración de problema	<p>¿Cuáles son los síntomas del problema? ¿Cuándo comenzó el problema? ¿Ocurre de manera sistemática o intermitente? Si es intermitente, ¿qué veces ha ocurrido?</p> <p>"Definición del problema"</p>
Evaluación del impacto	<p>¿Cuál es la gravedad del problema? ¿Cómo afecta a la aplicación cliente?</p> <ul style="list-style-type: none">• ¿Se ha conectado el cliente correctamente anteriormente?• ¿El cliente puede procesar, recuperar y eliminar datos?
ID del sistema StorageGRID	Seleccione Mantenimiento > sistema > Licencia . El ID del sistema de StorageGRID se muestra como parte de la licencia actual.
Versión de software	Haga clic en Ayuda > Acerca de para ver la versión de StorageGRID.
Personalización	<p>Resuma cómo se configura el sistema StorageGRID. Por ejemplo, enumere lo siguiente:</p> <ul style="list-style-type: none">• ¿El grid utiliza compresión de almacenamiento, cifrado de almacenamiento o cumplimiento de normativas?• ¿Hace ILM objetos replicados o codificados de borrado? ¿Garantiza ILM la redundancia de sitios? ¿Las reglas de ILM usan los comportamientos de ingesta estrictos, equilibrados o dobles?

✓	Elemento	Notas
	Registrar archivos y datos del sistema	<p>Recopile archivos de registro y datos del sistema para su sistema. Seleccione Soporte > Herramientas > registros.</p> <p>Es posible recopilar registros de toda la cuadrícula o de los nodos seleccionados.</p> <p>Si va a recopilar registros solo para los nodos seleccionados, asegúrese de incluir al menos un nodo de almacenamiento que tenga el servicio ADC. (Los tres primeros nodos de almacenamiento de un sitio incluyen el servicio ADC).</p> <p>"Recogida de archivos de registro y datos del sistema"</p>
	Información de línea de base	<p>Recopile información de la línea de base sobre las operaciones de ingesta, las operaciones de recuperación y el consumo de almacenamiento.</p> <p>"Establecimiento de líneas base"</p>
	Cronología de los cambios recientes	<p>Crear una línea de tiempo que resume los cambios recientes realizados en el sistema o en su entorno.</p> <p>"Crear una línea de tiempo de cambios recientes"</p>
	Historia de los esfuerzos para diagnosticar el problema	<p>Si ha tomado medidas para diagnosticar o solucionar el problema por su cuenta, asegúrese de registrar los pasos que ha realizado y el resultado.</p>

Información relacionada

["Administre StorageGRID"](#)

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

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.

Acercas 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 oculten 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.

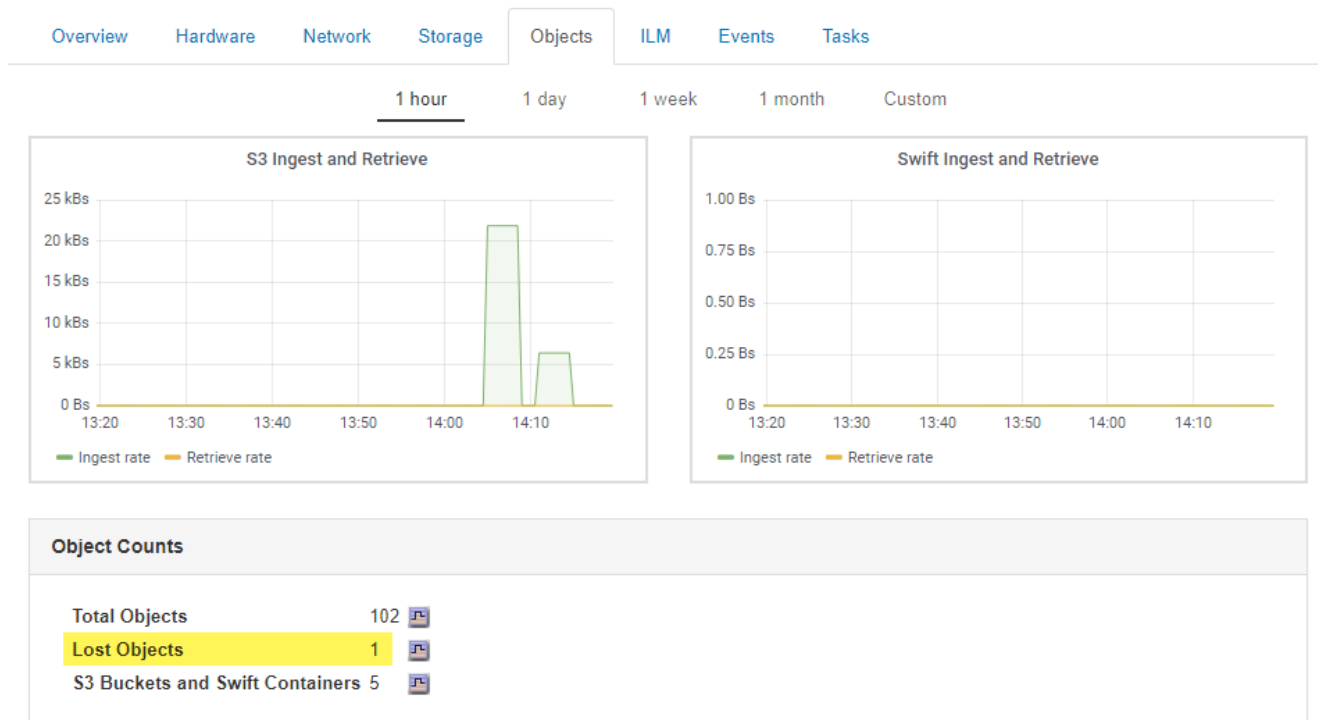
Investigue inmediatamente las alarmas o alertas de objetos perdidos. Es posible que deba tomar medidas para evitar la pérdida de datos adicional. En algunos casos, es posible que pueda restaurar un objeto perdido si realiza una acción rápida.

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",
    "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"
  }
}

```



```
]
}
```

- 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

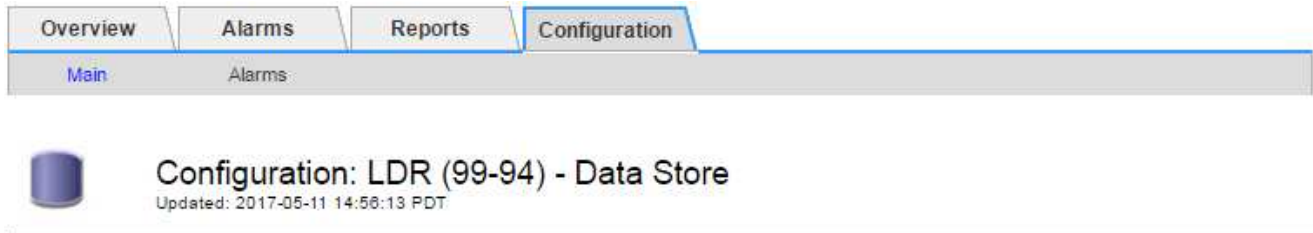
Puede restablecer el contador objetos perdidos desde cualquiera de las siguientes páginas:

- **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**.



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

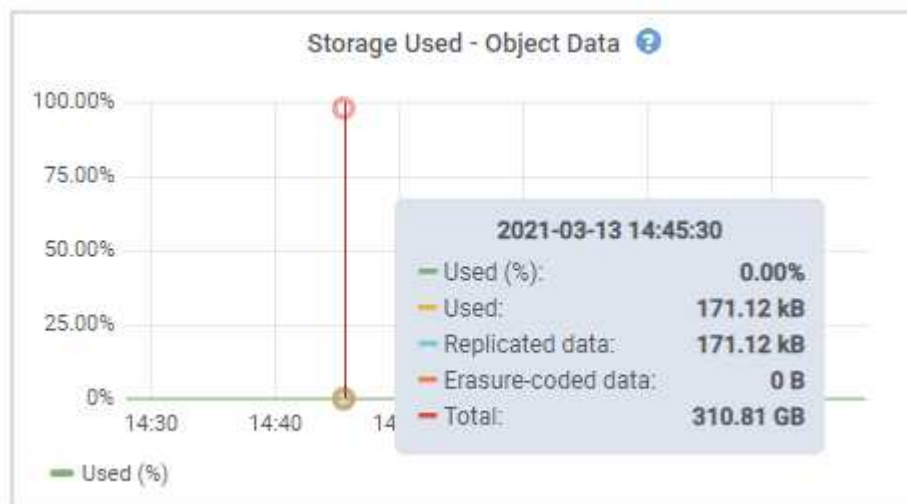
4. Seleccione **Nodes > Storage Node o Site > Storage**.

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.

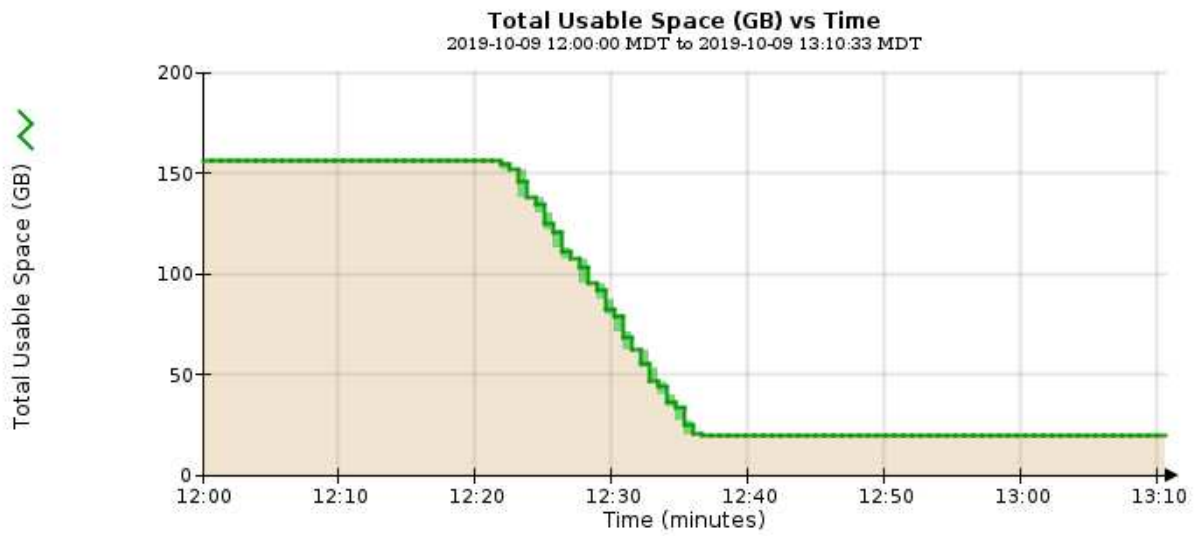
En este ejemplo, el espacio útil total cayó de aproximadamente 155 GB a 12:00 a 20 GB a 12:35, lo que corresponde al tiempo en que se activó la alarma DE SST.



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

Update




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

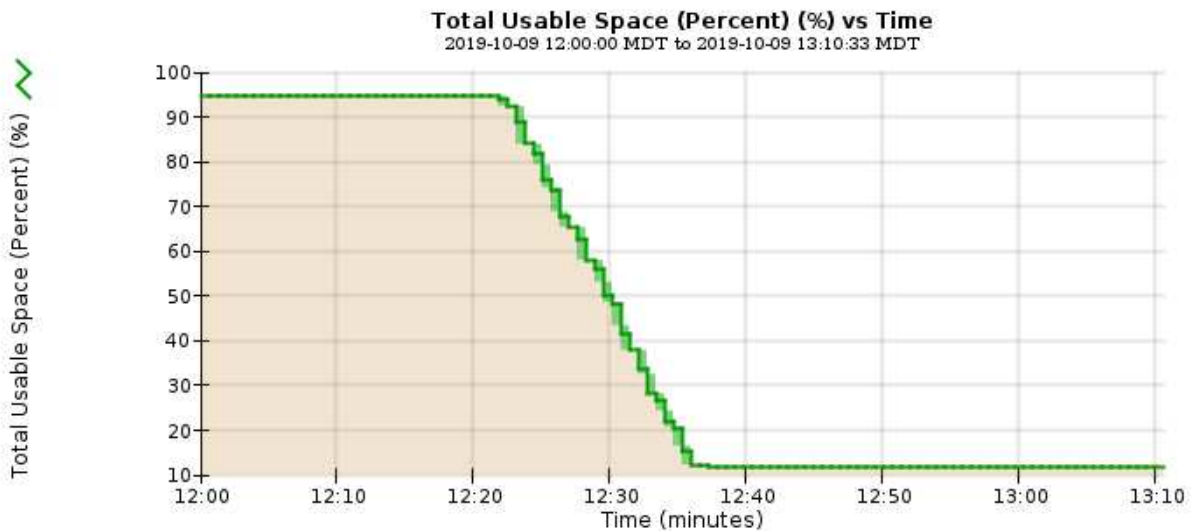
En este ejemplo, el espacio total utilizable cayó de un 95% a algo más de un 10% aproximadamente al mismo tiempo.

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"](#)

Resolución de problemas de metadatos

Existen varias tareas que se pueden realizar para determinar el origen de los problemas de metadatos.

Solución de problemas de la alerta de almacenamiento de metadatos bajos

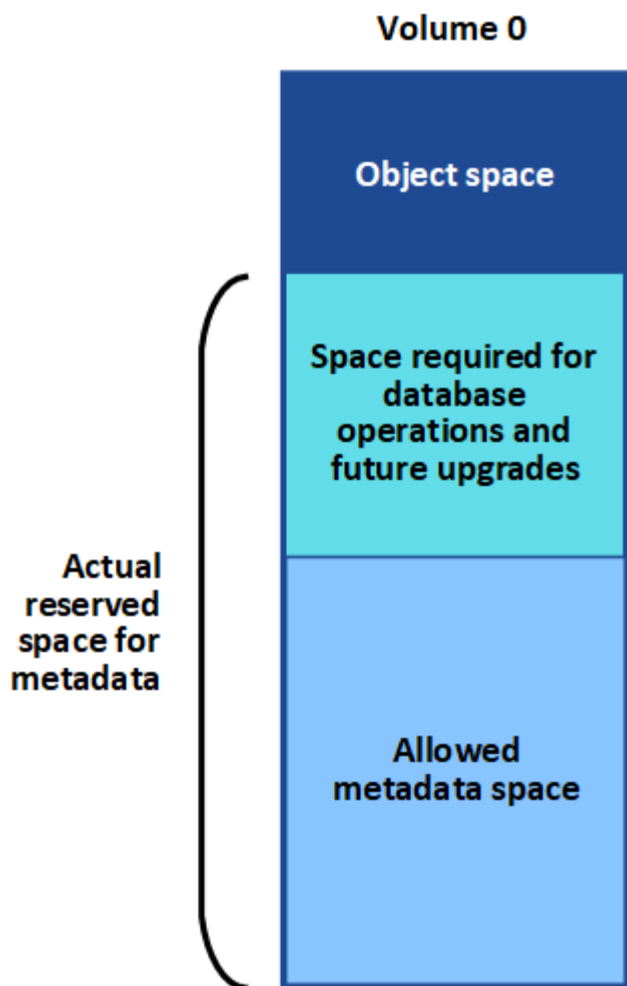
Si se activa la alerta **almacenamiento de metadatos bajo**, debe agregar nuevos nodos de almacenamiento.

Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

Acerca de esta tarea

StorageGRID reserva una cierta cantidad de espacio en el volumen 0 de cada nodo de almacenamiento para los metadatos del objeto. Este espacio se conoce como el espacio reservado real y se subdivide en el espacio permitido para los metadatos del objeto (el espacio de metadatos permitido) y el espacio necesario para las operaciones esenciales de la base de datos, como la compactación y la reparación. El espacio de metadatos permitido rige la capacidad general del objeto.



Si los metadatos de los objetos consumen más del 100% del espacio permitido para los metadatos, las operaciones de base de datos no se pueden ejecutar de forma eficiente y se producirán errores.

StorageGRID utiliza la siguiente métrica Prometheus para medir lo completo que está el espacio de metadatos permitido:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

Cuando esta expresión Prometheus alcanza ciertos umbrales, se activa la alerta **almacenamiento de metadatos bajo**.

- **Menor**: Los metadatos de objetos utilizan un 70% o más del espacio de metadatos permitido. Debe añadir nuevos nodos de almacenamiento Lo antes posible..
- **Mayor**: Los metadatos de objetos utilizan un 90% o más del espacio de metadatos permitido. Debe añadir nodos de almacenamiento nuevos inmediatamente.



Cuando los metadatos de objetos utilizan un 90 % o más del espacio de metadatos permitido, se muestra una advertencia en la consola. Si se muestra esta advertencia, debe añadir nodos de almacenamiento nuevos inmediatamente. Nunca debe permitir que los metadatos de objetos utilicen más de un 100 % del espacio permitido.

- **Crítico:** Los metadatos de objetos utilizan un 100% o más del espacio de metadatos permitido y están empezando a consumir el espacio necesario para las operaciones esenciales de la base de datos. Debe detener la ingesta de objetos nuevos y, inmediatamente, añadir nodos de almacenamiento nuevos.

En el ejemplo siguiente, los metadatos de objetos usan más del 100% del espacio de metadatos permitido. Ésta es una situación crítica, que dará como resultado errores y operaciones de la base de datos ineficientes.

The following Storage Nodes are using more than 90% of the space allowed for object metadata:

Node	% Used	Used	Allowed
DC1-S2-227	104.51%	6.73 GB	6.44 GB
DC1-S3-228	104.36%	6.72 GB	6.44 GB
DC2-S2-233	104.20%	6.71 GB	6.44 GB
DC1-S1-226	104.20%	6.71 GB	6.44 GB
DC2-S3-234	103.43%	6.66 GB	6.44 GB

Undesirable results can occur if object metadata uses more than 100% of the allowed space. You must add new Storage Nodes immediately or contact support.



Si el tamaño del volumen 0 es menor que la opción de almacenamiento de espacio reservado de metadatos (por ejemplo, en un entorno que no es de producción), el cálculo de la alerta **almacenamiento de metadatos bajo** podría ser inexacto.

Pasos

1. Seleccione **Alertas > corriente**.
2. En la tabla de alertas, expanda el grupo de alertas **almacenamiento de metadatos bajo**, si es necesario, y seleccione la alerta específica que desea ver.
3. Revise los detalles en el cuadro de diálogo de alertas.
4. Si se ha activado una alerta de **almacenamiento de metadatos bajo** importante o crítica, realice una ampliación para añadir nodos de almacenamiento inmediatamente.



Dado que StorageGRID mantiene copias completas de todos los metadatos de objetos en cada sitio, la capacidad de metadatos del grid completo está limitada por la capacidad de metadatos del sitio más pequeño. Si necesita añadir capacidad de metadatos a un sitio, también debe expandir otros sitios según el mismo número de nodos de almacenamiento.

Después de realizar la ampliación, StorageGRID redistribuye los metadatos de objetos existentes a los nodos nuevos, lo que aumenta la capacidad de metadatos general del grid. No se requiere ninguna acción del usuario. Se borra la alerta **almacenamiento de metadatos bajo**.

Información relacionada

["Supervisar la capacidad de metadatos de los objetos para cada nodo de almacenamiento"](#)

["Amplíe su grid"](#)

Solución de problemas de la alarma Servicios: Estado - Cassandra (SVST)

La alarma Servicios: Status - Cassandra (SVST) indica que es posible que deba reconstruir la base de datos de Cassandra para un nodo de almacenamiento. Cassandra se usa como almacén de metadatos para StorageGRID.

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

Si Cassandra se detiene durante más de 15 días (por ejemplo, el nodo de almacenamiento está apagado), Cassandra no se iniciará cuando el nodo se vuelva a conectar. Debe reconstruir la base de datos de Cassandra para el servicio DDS afectado.

Puede utilizar la página Diagnósticos para obtener información adicional sobre el estado actual de la cuadrícula.

"Ejecución de diagnósticos"



Si dos o más de los servicios de base de datos de Cassandra están inactivos durante más de 15 días, póngase en contacto con el soporte técnico y no continúe con los pasos a continuación.

Pasos

1. Seleccione **Soporte > Herramientas > Topología de cuadrícula**.
2. Seleccione **site > Storage Node > SSM > Servicios > Alarmas > Principal** para mostrar alarmas.

Este ejemplo muestra que se ha activado la alarma SVST.

Severity	Attribute	Description	Alarm Time	Trigger Value	Current Value	Acknowledge Time	Acknowledge
Minor	SVST (Services: Status - Cassandra)	Not Running	2014-08-14 14:56:28 PDT	Not Running	Not Running		<input type="checkbox"/>

La página principal de los servicios de SSM también indica que Cassandra no se está ejecutando.

Overview
Alarms
Reports
Configuration

Main

Overview: SSM (DC2-S1) - Services

Updated: 2017-03-30 09:53:53 MDT

Operating System: Linux
3.16.0-4-amd64

Services

Service	Version	Status	Threads	Load	Memory
Account Service	10.4.0-20161224.0333.803cd91	Running	7	0.002 %	12 MB
Administrative Domain Controller (ADC)	10.4.0-20170329.0039.8800cae	Running	52	0.14 %	63.1 MB
Cassandra	4.6.12-1.byc.0-20170308.0109.ba3598a	Not Running	0	0 %	0 B
Content Management System (CMS)	10.4.0-20170220.1846.1a76aed	Running	18	0.055 %	20.6 MB
Distributed Data Store (DDS)	10.4.0-20170329.0039.8800cae	Running	104	1.301 %	76 MB
Identity Service	10.4.0-20170203.2038.a457d45	Running	6	0 %	8.75 MB
Keystone Service	10.4.0-20170104.1815.6e52138	Running	5	0 %	7.77 MB
Local Distribution Router (LDR)	10.4.0-20170329.0039.8800cae	Running	109	0.218 %	96.6 MB
Server Manager	10.4.0-20170306.2303.9649faf	Running	4	3.58 %	19.1 MB

1. Intente reiniciar Cassandra desde el nodo de almacenamiento:

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. Introduzca: `/etc/init.d/cassandra status`

c. Si Cassandra no se está ejecutando, reinicie: `/etc/init.d/cassandra restart`

2. Si Cassandra no se reinicia, determine cuánto tiempo ha estado inactivo Cassandra. Si Cassandra ha estado inactiva durante más de 15 días, debe reconstruir la base de datos de Cassandra.



Si dos o más de los servicios de base de datos de Cassandra están inactivos, póngase en contacto con el soporte técnico y no continúe con los pasos que se indican a continuación.

Puede determinar cuánto tiempo ha estado inactivo Cassandra trazando una entrada de datos o revisando el archivo `servermanager.log`.

3. Para crear un gráfico en Cassandra:

a. Seleccione **Soporte > Herramientas > Topología de cuadrícula**. A continuación, seleccione **site > Storage Node > SSM > Servicios > Informes > Cartas**.

b. Seleccione **atributo > Servicio: Estado - Cassandra**.

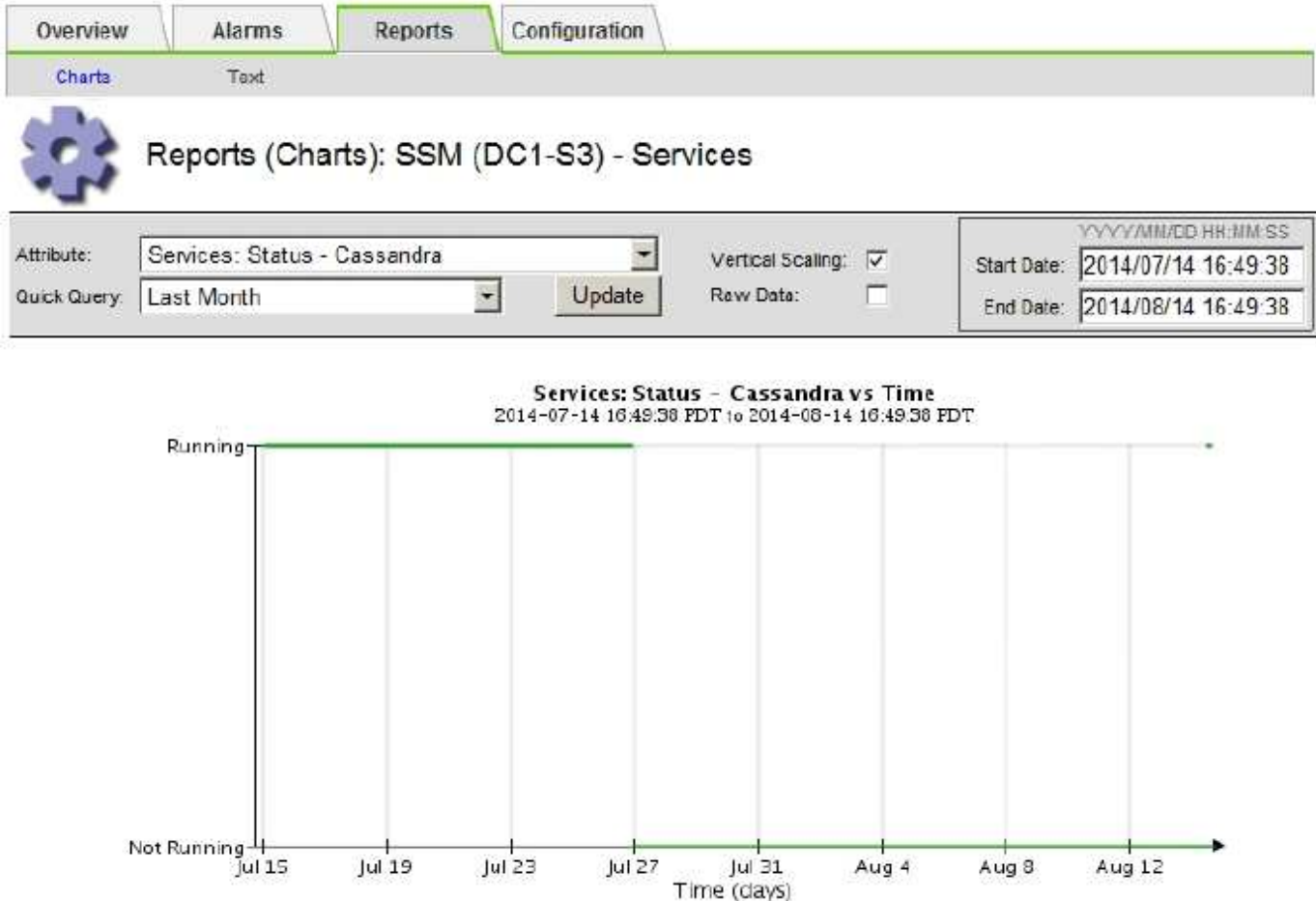
c. Para **Fecha de inicio**, introduzca una fecha que tenga al menos 16 días antes de la fecha actual. Para

Fecha de finalización, introduzca la fecha actual.

d. Haga clic en **Actualizar**.

e. Si el gráfico muestra que Cassandra está inactiva durante más de 15 días, vuelva a generar la base de datos de Cassandra.

El siguiente ejemplo de gráfico muestra que Cassandra ha estado inactiva durante al menos 17 días.



1. Para revisar el archivo `servermanager.log` en el nodo de almacenamiento:

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. Introduzca: `cat /var/local/log/servermanager.log`

Se muestra el contenido del archivo `servermanager.log`.

Si Cassandra ha estado inactiva durante más de 15 días, se muestra el siguiente mensaje en el archivo `servermanager.log`:


```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

- a. Asegúrese de que la Marca de hora de este mensaje sea la hora a la que intentó reiniciar Cassandra como se indica en el paso [Reinicie Cassandra desde el nodo de almacenamiento](#).

Puede haber más de una entrada para Cassandra; debe encontrar la entrada más reciente.

- b. Si Cassandra ha estado inactiva durante más de 15 días, debe reconstruir la base de datos de Cassandra.

Para obtener instrucciones, consulte «"recuperación desde un único nodo de almacenamiento en menos de 15 días" en las instrucciones de recuperación y mantenimiento.

- c. Póngase en contacto con el soporte técnico si las alarmas no se borran después de reconstruir Cassandra.

Información relacionada

["Mantener recuperar"](#)

Solución de errores de Cassandra fuera de memoria (alarma SMTT)

Se activa una alarma total Events (SMTT) cuando la base de datos de Cassandra tiene un error de falta de memoria. Si se produce este error, póngase en contacto con el soporte técnico para solucionar el problema.

Acerca de esta tarea

Si se produce un error de falta de memoria en la base de datos de Cassandra, se crea un volcado de pila, se activa una alarma Eventos totales (SMTT) y el recuento de errores de memoria de Cassandra se incrementa en uno.

Pasos

1. Para ver el evento, seleccione **Nodes > grid node > Events**.
2. Compruebe que el número de errores de memoria de salida de Cassandra sea 1 o superior.

Puede utilizar la página Diagnósticos para obtener información adicional sobre el estado actual de la cuadrícula.

["Ejecución de diagnósticos"](#)

3. Vaya a `/var/local/core/`, comprima el `Cassandra.hprof` y envíelo al soporte técnico.
4. Haga una copia de seguridad del `Cassandra.hprof` y elimínelo del `/var/local/core/` directory.

Este archivo puede tener un tamaño de hasta 24 GB, por lo que debe eliminarlo para liberar espacio.

5. Una vez resuelto el problema, haga clic en **Restablecer recuentos de eventos**.



Para restablecer los recuentos de eventos, debe tener el permiso Configuración de página de topología de cuadrícula.

Información relacionada

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

Solución de errores de certificado

Si ve un problema de seguridad o un certificado cuando intenta conectarse a StorageGRID mediante un explorador web, un cliente S3 o Swift o una herramienta de supervisión externa, debe comprobar el certificado.

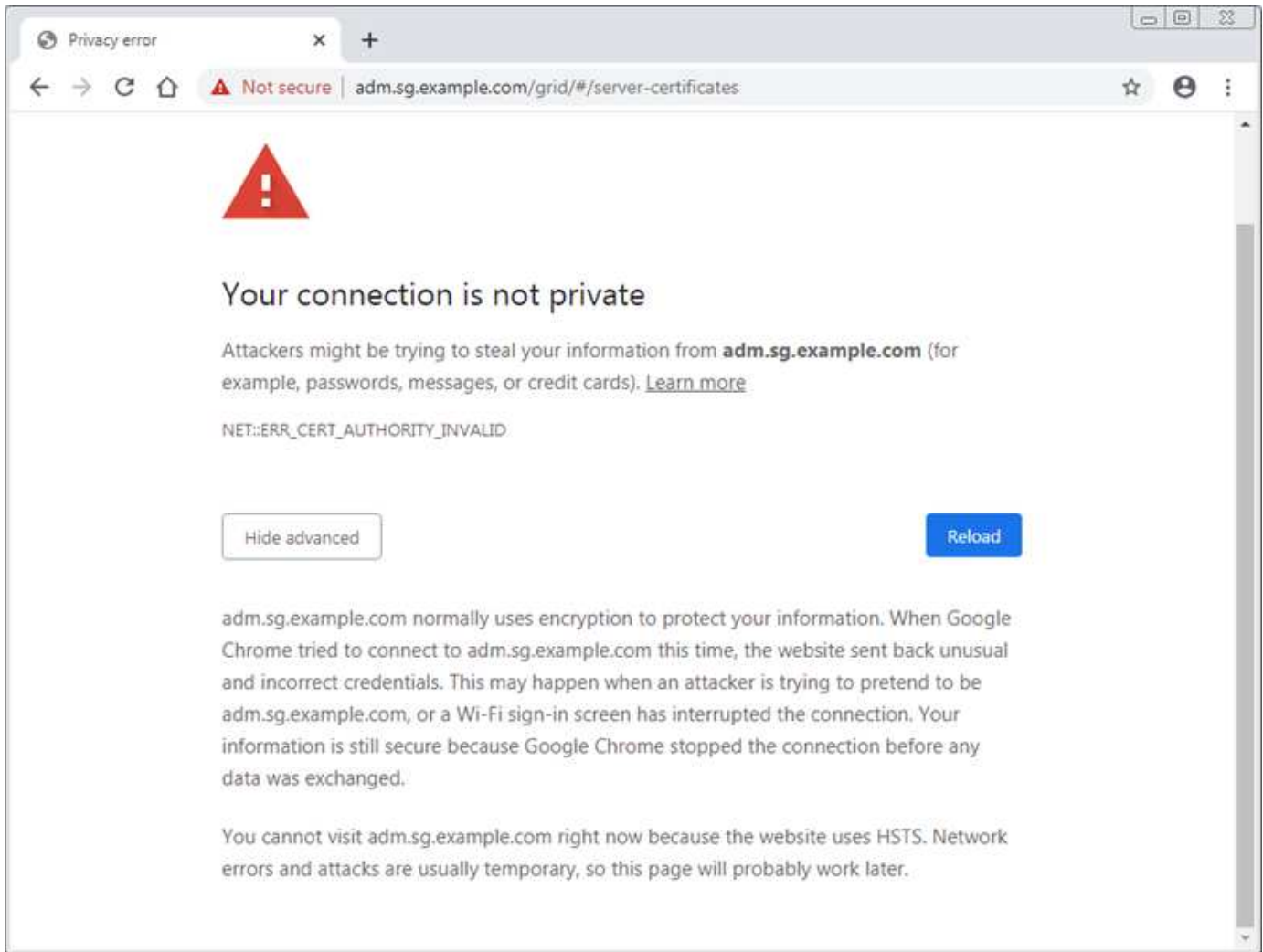
Acerca de esta tarea

Los errores de certificado pueden causar problemas al intentar conectarse a StorageGRID mediante el Administrador de grid, la API de gestión de grid, el Administrador de inquilinos o la API de gestión de inquilinos. También se pueden producir errores de certificado cuando se intenta conectar con un cliente S3 o Swift o una herramienta de supervisión externa.

Si accede a Grid Manager o a Intenant Manager utilizando un nombre de dominio en lugar de una dirección IP, el explorador mostrará un error de certificado sin una opción para omitir si se produce alguna de las siguientes situaciones:

- El certificado del servidor de la interfaz de gestión personalizada caduca.
- Se revierte de un certificado del servidor de interfaz de gestión personalizado al certificado de servidor predeterminado.

En el ejemplo siguiente se muestra un error de certificado cuando expiró el certificado del servidor de interfaz de gestión personalizado:



Para asegurarse de que las operaciones no se ven interrumpidas por un certificado de servidor con errores, la alerta **caducidad del certificado de servidor para la interfaz de administración** se activa cuando el certificado de servidor está a punto de caducar.

Cuando se utilizan certificados de cliente para la integración de Prometheus externa, los errores de certificado pueden producirse por el certificado del servidor de la interfaz de gestión de StorageGRID o por certificados de cliente. La alerta **caducidad de los certificados configurados en la página certificados de cliente** se activa cuando un certificado de cliente está a punto de caducar.

Pasos

1. Si ha recibido una notificación de alerta sobre un certificado caducado, acceda a los detalles del certificado:
 - Para un certificado de servidor, seleccione **Configuración > Configuración de red > certificados de servidor**.
 - Para un certificado de cliente, seleccione **Configuración > Control de acceso > certificados de cliente**.
2. Compruebe el período de validez del certificado.

Algunos exploradores web y clientes S3 o Swift no aceptan certificados con un período de validez superior a 398 días.

3. Si el certificado ha caducado o lo hará pronto, cargue o genere uno nuevo.

- Para obtener un certificado de servidor, consulte los pasos para configurar un certificado de servidor personalizado para el Administrador de grid y el Administrador de inquilinos en las instrucciones para administrar StorageGRID.
 - Para obtener un certificado de cliente, consulte los pasos para configurar un certificado de cliente en las instrucciones para administrar StorageGRID.
4. En el caso de errores de certificado de servidor, intente con una de las siguientes opciones o ambas:
- Asegúrese de que se rellena el asunto Nombre alternativo (SAN) del certificado y que LA SAN coincida con la dirección IP o el nombre de host del nodo al que se conecta.
 - Si está intentando conectarse a StorageGRID con un nombre de dominio:
 - i. Introduzca la dirección IP del nodo de administración en lugar del nombre de dominio para omitir el error de conexión y acceder a Grid Manager.
 - ii. En Grid Manager, seleccione **Configuración > Configuración de red > certificados de servidor** para instalar un nuevo certificado personalizado o continúe con el certificado predeterminado.
 - iii. En las instrucciones para administrar StorageGRID, consulte los pasos para configurar un certificado de servidor personalizado para el Administrador de grid y el Administrador de inquilinos.

Información relacionada

["Administre StorageGRID"](#)

Solucionar problemas del nodo de administrador y de la interfaz de usuario

Existen varias tareas que se pueden realizar para determinar el origen de los problemas relacionados con los nodos de administrador y la interfaz de usuario de StorageGRID.

Solución de problemas de errores de inicio de sesión

Si se produce un error al iniciar sesión en un nodo de administrador de StorageGRID, es posible que el sistema tenga un problema con la configuración de la federación de identidades, un problema de red o de hardware, un problema con los servicios del nodo de administrador o un problema con la base de datos Cassandra en los nodos de almacenamiento conectados.

Lo que necesitará

- Debe tener la `Passwords.txt` archivo.
- Debe tener permisos de acceso específicos.

Acerca de esta tarea

Use estas directrices de solución de problemas si ve alguno de los siguientes mensajes de error al intentar iniciar sesión en un nodo de administrador:

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start...`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page...`

Pasos

1. Espere 10 minutos e intente iniciar sesión de nuevo.

Si el error no se resuelve automáticamente, vaya al siguiente paso.

2. Si el sistema StorageGRID tiene más de un nodo de administración, intente iniciar sesión en el Administrador de grid desde otro nodo de administración.
 - Si puede iniciar sesión, puede utilizar las opciones **Panel**, **nodos**, **Alertas** y **Soporte** para ayudar a determinar la causa del error.
 - Si solo tiene un nodo de administrador o aún no puede iniciar sesión, vaya al siguiente paso.
3. Determine si el hardware del nodo está sin conexión.
4. Si el inicio de sesión único (SSO) está habilitado para el sistema StorageGRID, consulte los pasos para configurar el inicio de sesión único, en las instrucciones para administrar StorageGRID.

Es posible que deba deshabilitar y volver a habilitar temporalmente el inicio de la sesión único para un nodo de administración a fin de resolver cualquier problema.



Si SSO está habilitado, no puede iniciar sesión mediante un puerto restringido. Se debe usar el puerto 443.

5. Determine si la cuenta que está utilizando pertenece a un usuario federado.

Si la cuenta de usuario federada no funciona, intente iniciar sesión en Grid Manager como un usuario local, como root.

- Si el usuario local puede iniciar sesión:
 - i. Revise las alarmas mostradas.
 - ii. Seleccione **Configuración > Federación de identidades**.
 - iii. Haga clic en **probar conexión** para validar la configuración de conexión para el servidor LDAP.
 - iv. Si la prueba falla, resuelva cualquier error de configuración.
 - Si el usuario local no puede iniciar sesión y está seguro de que las credenciales son correctas, vaya al paso siguiente.
6. Utilice Secure Shell (ssh) para iniciar sesión en el nodo de administración:
 - a. Introduzca el siguiente comando: `ssh admin@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 #.

7. Consulte el estado de todos los servicios que se ejecutan en el nodo de grid: `storagegrid-status`

Asegúrese de que los servicios de nms, mi, nginx y API de gestión están funcionando.

La salida se actualiza inmediatamente si el estado de un servicio cambia.

```

$ storagegrid-status
Host Name                99-211
IP Address               10.96.99.211
Operating System Kernel  4.19.0                 Verified
Operating System Environment Debian 10.1             Verified
StorageGRID Webscale Release 11.4.0                 Verified
Networking                Verified
Storage Subsystem        Verified
Database Engine           5.5.9999+default      Running
Network Monitoring       11.4.0                 Running
Time Synchronization     1:4.2.8p10+dfsg      Running
ams                       11.4.0                 Running
cmn                       11.4.0                 Running
nms                       11.4.0                 Running
ssm                       11.4.0                 Running
mi                       11.4.0                 Running
dynip                    11.4.0                 Running
nginx                    1.10.3                 Running
tomcat                   9.0.27                 Running
grafana                  6.4.3                  Running
mgmt api                 11.4.0                 Running
prometheus               11.4.0                 Running
persistence              11.4.0                 Running
ade exporter             11.4.0                 Running
alertmanager             11.4.0                 Running
attrDownPurge            11.4.0                 Running
attrDownSamp1            11.4.0                 Running
attrDownSamp2            11.4.0                 Running
node exporter            0.17.0+ds              Running
sg snmp agent            11.4.0                 Running

```

8. Confirme que el servidor web de Apache se está ejecutando: # `service apache2 status`

1. Utilice Lumberjack para recopilar registros: # `/usr/local/sbin/lumberjack.rb`

Si la autenticación fallida se ha producido en el pasado, puede utilizar las opciones de script `--start` y `--end` Lumberjack para especificar el intervalo de tiempo adecuado. Utilice `luberjack -h` para obtener más información sobre estas opciones.

La salida al terminal indica dónde se ha copiado el archivo de registro.

1. Revise los siguientes registros:

- `/var/local/log/bycast.log`
- `/var/local/log/bycast-err.log`
- `/var/local/log/nms.log`

- `**/*commands.txt`

2. Si no pudo identificar ningún problema con el nodo de administración, ejecute cualquiera de los siguientes comandos para determinar las direcciones IP de los tres nodos de almacenamiento que ejecutan el servicio ADC en el sitio. Normalmente, estos son los primeros tres nodos de almacenamiento que se instalaron en el sitio.

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

Los nodos de administración usan el servicio ADC durante el proceso de autenticación.

3. Desde el nodo de administración, inicie sesión en cada uno de los nodos de almacenamiento de ADC usando las direcciones IP identificadas.
 - a. Introduzca el siguiente comando: `ssh admin@grid_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 `#`.

4. Consulte el estado de todos los servicios que se ejecutan en el nodo de grid: `storagegrid-status`
Asegúrese de que los servicios `idnt`, `acct`, `nginx` y `cassandra` están en ejecución.
5. Repita los pasos [Utilice Lumberjack para recopilar registros](#) y.. [Revisar los registros](#) Para revisar los registros en los nodos de almacenamiento.
6. Si no puede resolver el problema, póngase en contacto con el soporte técnico.

Proporcione los registros recopilados al soporte técnico.

Información relacionada

["Administre StorageGRID"](#)

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

Solucionar problemas de la interfaz de usuario

Es posible que vea problemas con el administrador de grid o el administrador de inquilinos después de actualizar a una nueva versión del software StorageGRID.

La interfaz Web no responde de la manera esperada

Es posible que el administrador de grid o el administrador de inquilinos no respondan como se espera después de actualizar el software StorageGRID.

Si tiene problemas con la interfaz web:

- Asegúrese de utilizar un navegador compatible.



La compatibilidad con el explorador ha cambiado para StorageGRID 11.5. Confirme que está utilizando una versión compatible.

- Borre la caché del navegador web.

Al borrar la caché se eliminan los recursos obsoletos utilizados por la versión anterior del software StorageGRID y se permite que la interfaz de usuario vuelva a funcionar correctamente. Para obtener instrucciones, consulte la documentación de su navegador web.

Información relacionada

["Requisitos del navegador web"](#)

["Administre StorageGRID"](#)

Comprobar el estado de un nodo administrador no disponible

Si el sistema StorageGRID incluye varios nodos de administrador, puede usar otro nodo de administración para comprobar el estado de un nodo de administración no disponible.

Lo que necesitará

Debe tener permisos de acceso específicos.

Pasos

1. Desde un nodo de administración disponible, inicie sesión en Grid Manager utilizando un explorador compatible.
2. Seleccione **Soporte > Herramientas > Topología de cuadrícula**.
3. Seleccione **Sitio > nodo de administración no disponible > SSM > Servicios > Descripción general > Principal**.
4. Busque servicios con el estado no en ejecución y que también puedan mostrarse en azul.



Overview: SSM (MM-10-224-4-81-ADM1) - Services

Updated: 2017-01-27 11:52:51 EST

Operating System: Linux
3.16.0-4-amd64

Services

Service	Version	Status	Threads	Load	Memory
Audit Management System (AMS)	10.4.0-20170113.2207.3ec2cd0	Running	52	0.043 %	35.7 MB
CIFS Filesharing (nmbd)	2:4.2.14+dfsg-0+deb8u2	Running	1	0 %	5.5 MB
CIFS Filesharing (smbd)	2:4.2.14+dfsg-0+deb8u2	Running	1	0 %	14.5 MB
CIFS Filesharing (winbindd)	2:4.2.14+dfsg-0+deb8u2	Not Running	0	0 %	0 B
Configuration Management Node (CMN)	10.4.0-20170113.2207.3ec2cd0	Running	52	0.055 %	41.3 MB
Database Engine	5.5.53-0+deb8u1	Running	47	0.354 %	1.33 GB
Grid Deployment Utility Server	10.4.0-20170112.2125.c4253bb	Running	3	0 %	32.8 MB
Management Application Program Interface (mgmt-api)	10.4.0-20170113.2136.07c4997	Not Running	0	0 %	0 B
NFS Filesharing	10.4.0-20161224.0333.803cd91	Not Running	0	0 %	0 B
NMS Data Cleanup	10.4.0-20161224.0333.803cd91	Running	22	0.008 %	52.4 MB
NMS Data Downsampler 1	10.4.0-20161224.0333.803cd91	Running	22	0.049 %	195 MB
NMS Data Downsampler 2	10.4.0-20161224.0333.803cd91	Running	22	0.009 %	157 MB
NMS Processing Engine	10.4.0-20161224.0333.803cd91	Running	40	0.132 %	200 MB

- Determine si las alarmas se han activado.
- Realice las acciones adecuadas para resolver el problema.

Información relacionada

["Administre StorageGRID"](#)

Resolución de problemas de red, hardware y plataforma

Existen varias tareas que puede realizar para ayudar a determinar el origen de los problemas relacionados con la red, el hardware y la plataforma de StorageGRID.

Resolución de problemas de errores "'422: Entidad no procesable''

El error 422: Entidad no procesable puede ocurrir en varias circunstancias. Compruebe el mensaje de error para determinar la causa del problema.

Si ve uno de los mensajes de error de la lista, realice la acción recomendada.

Mensaje de error	Causa raíz y acción correctiva
<pre>422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839</pre>	<p>Este mensaje puede aparecer si selecciona la opción no utilizar TLS para Seguridad de la capa de transporte (TLS) al configurar la federación de identidades mediante Active Directory de Windows (AD).</p> <p>El uso de la opción no usar TLS no es compatible con servidores AD que aplican la firma LDAP. Debe seleccionar la opción Use STARTTLS o la opción Use LDAPS para TLS.</p>
<pre>422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)</pre>	<p>Este mensaje aparece si intenta utilizar un cifrado no compatible para establecer una conexión TLS (Seguridad de la capa de transporte) desde StorageGRID a un sistema externo utilizado para identificar los grupos de almacenamiento de la federación o de la nube.</p> <p>Compruebe los códigos que ofrece el sistema externo. El sistema debe usar uno de los cifrados compatibles con StorageGRID para conexiones TLS salientes, tal y como se muestra en las instrucciones para administrar StorageGRID.</p>

Información relacionada

["Administre StorageGRID"](#)

Solución de problemas de la alerta de discrepancia de MTU de red de cuadrícula

La alerta **Red Grid MTU mismatch** se activa cuando la configuración de la unidad de transmisión máxima (MTU) para la interfaz Red Grid (eth0) difiere significativamente entre los nodos de la cuadrícula.

Acerca de esta tarea

Las diferencias en la configuración de MTU podrían indicar que algunas redes eth0, pero no todas, están

configuradas para tramas gigantes. Un error de coincidencia del tamaño de MTU de más de 1000 puede provocar problemas de rendimiento de la red.

Pasos

1. Enumere la configuración de MTU para eth0 en todos los nodos.
 - Utilice la consulta proporcionada en Grid Manager.
 - Vaya a `primary Admin Node IP address/metrics/graph` e introduzca la siguiente consulta: `node_network_mtu_bytes{interface='eth0'}`
2. Modifique la configuración de MTU según sea necesario para asegurarse de que son la misma para la interfaz de red de cuadrícula (eth0) en todos los nodos.
 - Para los nodos del dispositivo, consulte las instrucciones de instalación y mantenimiento del dispositivo.
 - Para los nodos basados en Linux y VMware, use el siguiente comando: `/usr/sbin/change-mtu.py [-h] [-n node] mtu network [network...]`

Ejemplo: `change-mtu.py -n node 1500 grid admin`

Nota: En los nodos basados en Linux, si el valor de MTU deseado para la red en el contenedor supera el valor ya configurado en la interfaz del host, primero debe configurar la interfaz del host para que tenga el valor de MTU deseado y luego utilice `change-mtu.py` Script para cambiar el valor MTU de la red en el contenedor.

Use los siguientes argumentos para modificar la MTU en los nodos basados en Linux o VMware.

Argumentos posicionales	Descripción
mtu	La MTU que se va a establecer. Debe estar entre 1280 y 9216.
network	Las redes a las que se va a aplicar la MTU. Incluya uno o varios de los siguientes tipos de red: <ul style="list-style-type: none"> • cuadrícula • admin • cliente

+

Argumentos opcionales	Descripción
<code>-h, - help</code>	Muestra el mensaje de ayuda y sale.
<code>-n node, --node node</code>	El nodo. El valor predeterminado es el nodo local.

Información relacionada

["SG100 servicios de aplicaciones SG1000"](#)

"Dispositivos de almacenamiento SG6000"

"Dispositivos de almacenamiento SG5700"

"Dispositivos de almacenamiento SG5600"

Solución de problemas de la alarma error de recepción de red (NRER)

Las alarmas de error de recepción de red (NRER) pueden deberse a problemas de conectividad entre StorageGRID y el hardware de red. En algunos casos, los errores del NRER pueden aclararse sin intervención manual. Si los errores no se borran, realice las acciones recomendadas.

Acerca de esta tarea

Las alarmas NRER pueden deberse a los siguientes problemas de hardware de red que se conecta a StorageGRID:

- Se requiere corrección de errores de reenvío (FEC) y no se utiliza
- Discrepancia entre el puerto del switch y la MTU de NIC
- Índices altos de errores de enlace
- Desbordamiento del búfer de anillo NIC

Pasos

1. Siga los pasos de solución de problemas para todas las posibles causas de la alarma NRER dada la configuración de la red.

- Si el error es causado por una discrepancia de FEC, realice los siguientes pasos:

Nota: Estos pasos sólo se aplican para los errores NRER causados por el discordancia de FEC en los dispositivos StorageGRID.

- i. Compruebe el estado de FEC del puerto en el interruptor conectado al dispositivo StorageGRID.
- ii. Compruebe la integridad física de los cables del aparato al interruptor.
- iii. Si desea cambiar los ajustes de FEC para intentar resolver la alarma NRER, asegúrese primero de que el dispositivo esté configurado para el modo **automático** en la página Configuración de vínculos del instalador de dispositivos StorageGRID (consulte las instrucciones de instalación y mantenimiento del dispositivo). A continuación, cambie la configuración de FEC en los puertos del switch. Los puertos del dispositivo StorageGRID ajustarán los ajustes del FEC para que coincidan, si es posible.

(No puede configurar los ajustes de FEC en dispositivos StorageGRID. En su lugar, los dispositivos intentan descubrir y duplicar los ajustes de FEC en los puertos de conmutador a los que están conectados. Si los enlaces se ven forzados a velocidades de red de 25-GbE o 100-GbE, es posible que el switch y la NIC no negocien una configuración de FEC común. Sin un ajuste FEC común, la red volverá al modo «no-FEC». Cuando el FEC no está activado, las conexiones son más susceptibles a errores causados por el ruido eléctrico.)

Nota: Los aparatos StorageGRID admiten FEC FIRECODE (FC) y Reed Solomon (RS), así como no FEC.

- Si el error se debe a un error de coincidencia entre un puerto del switch y una MTU de NIC, compruebe que el tamaño de MTU configurado en el nodo sea el mismo que la configuración de MTU para el puerto del switch.

El tamaño de MTU configurado en el nodo puede ser más pequeño que la configuración en el puerto del switch al que está conectado el nodo. Si un nodo StorageGRID recibe una trama de Ethernet mayor que su MTU, lo cual es posible con esta configuración, se podría notificar la alarma NRER. Si cree que esto es lo que está sucediendo, cambie la MTU del puerto del switch para que coincida con la MTU de la interfaz de red de StorageGRID o cambie la MTU de la interfaz de red de StorageGRID para que coincida con el puerto del switch, según sus objetivos o requisitos de MTU completos.



Para obtener el mejor rendimiento de red, todos los nodos deben configurarse con valores MTU similares en sus interfaces de Grid Network. La alerta **Red de cuadrícula MTU** se activa si hay una diferencia significativa en la configuración de MTU para la Red de cuadrícula en nodos individuales. Los valores de MTU no tienen que ser iguales para todos los tipos de red.



Para cambiar la configuración de MTU, consulte la guía de instalación y mantenimiento del dispositivo.

- Si el error se debe a unos altos índices de errores de enlace, realice los siguientes pasos:
 - i. Active FEC, si aún no está activado.
 - ii. Compruebe que el cableado de red es de buena calidad y que no está dañado o conectado incorrectamente.
 - iii. Si parece que los cables no son el problema, póngase en contacto con el soporte técnico.



Es posible que note altas tasas de error en un entorno con alto nivel de ruido eléctrico.

- Si el error es un desbordamiento del búfer de anillo NIC, póngase en contacto con el soporte técnico.

El búfer de anillo puede desbordarse cuando el sistema StorageGRID está sobrecargado y no puede procesar eventos de red de forma oportuna.

2. Después de resolver el problema subyacente, restablezca el contador de errores.
 - a. Seleccione **Soporte > Herramientas > Topología de cuadrícula**.
 - b. Seleccione **site > grid node > SSM > Recursos > Configuración > Principal**.
 - c. Seleccione **Restablecer recuento de errores de recepción** y haga clic en **aplicar cambios**.

Información relacionada

["Solución de problemas de la alerta de discrepancia de MTU de red de cuadrícula"](#)

["Referencia de alarmas \(sistema heredado\)"](#)

["Dispositivos de almacenamiento SG6000"](#)

["Dispositivos de almacenamiento SG5700"](#)

["Dispositivos de almacenamiento SG5600"](#)

["SG100 servicios de aplicaciones SG1000"](#)

Solución de problemas de errores de sincronización temporal

Es posible que observe problemas con la sincronización de la hora en la cuadrícula.

Si tiene problemas de sincronización temporal, compruebe que ha especificado al menos cuatro orígenes NTP externos, cada uno de los cuales proporciona una referencia estratum 3 o mejor, y que sus nodos StorageGRID pueden acceder a todas las fuentes NTP externas con normalidad.



Al especificar el origen NTP externo para una instalación StorageGRID de nivel de producción, no utilice el servicio de hora de Windows (W32Time) en una versión de Windows anterior a Windows Server 2016. El servicio de tiempo en versiones anteriores de Windows no es lo suficientemente preciso y no es compatible con Microsoft para su uso en entornos de gran precisión como StorageGRID.

Información relacionada

["Mantener recuperar"](#)

Linux: Problemas de conectividad de red

Es posible que vea problemas con la conectividad de red para los nodos grid StorageGRID alojados en hosts Linux.

Clonación de direcciones MAC

En algunos casos, los problemas de red se pueden resolver mediante la clonación de direcciones MAC. Si utiliza hosts virtuales, establezca el valor de la clave de clonación de direcciones MAC para cada una de las redes en "true" en el archivo de configuración del nodo. Este ajuste hace que la dirección MAC del contenedor StorageGRID utilice la dirección MAC del host. Para crear archivos de configuración de nodos, consulte las instrucciones de la guía de instalación de su plataforma.



Cree interfaces de red virtual independientes que utilice el sistema operativo del host Linux. Al utilizar las mismas interfaces de red para el sistema operativo host Linux y el contenedor StorageGRID, es posible que no se pueda acceder al sistema operativo del host si no se ha habilitado el modo promiscuo en el hipervisor.

Para obtener más información sobre cómo activar la clonación de MAC, consulte las instrucciones de la guía de instalación de la plataforma.

Modo promiscuo

Si no desea utilizar la clonación de direcciones MAC y, más bien, permite que todas las interfaces reciban y transmitan datos para direcciones MAC distintas a las asignadas por el hipervisor, asegúrese de que las propiedades de seguridad de los niveles de conmutador virtual y grupo de puertos están configuradas en **Aceptar** para modo promiscuous, cambios de dirección MAC y señales falsificadas. Los valores establecidos en el conmutador virtual pueden ser anulados por los valores en el nivel de grupo de puertos, por lo que asegúrese de que la configuración sea la misma en ambos lugares.

Información relacionada

["Instale Red Hat Enterprise Linux o CentOS"](#)

["Instalar Ubuntu o Debian"](#)

Linux: El estado del nodo es «'huérfano'».

Un nodo Linux en estado huérfano suele indicar que el servicio de StorageGRID o el demonio del nodo StorageGRID que controla el contenedor del nodo ha muerto inesperadamente.

Acerca de esta tarea

Si un nodo de Linux informa de que está en el estado huérfano, debería:

- Compruebe los registros en busca de errores y mensajes.
- Intente iniciar de nuevo el nodo.
- Si es necesario, utilice los comandos de Docker para detener el contenedor de nodos existente.
- Reinicie el nodo.

Pasos

1. Compruebe los registros del demonio de servicio y del nodo huérfano para ver errores o mensajes obvios acerca de salir inesperadamente.
2. Inicie sesión en el host como raíz o utilice una cuenta con permiso sudo.
3. Intente iniciar nuevamente el nodo ejecutando el siguiente comando: `$ sudo storagegrid node start node-name`

```
$ sudo storagegrid node start DC1-S1-172-16-1-172
```

Si el nodo está huérfano, la respuesta es

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. Desde Linux, detenga el contenedor Docker y cualquier proceso que controle los procesos del nodo storagegrid: `sudo docker stop --time secondscontainer-name`

Para `seconds`, introduzca el número de segundos que desea esperar a que se detenga el contenedor (normalmente 15 minutos o menos).

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. Reinicie el nodo: `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

Linux: Resolución de problemas de compatibilidad con IPv6

Es posible que deba habilitar la compatibilidad de IPv6 en el kernel si ha instalado nodos StorageGRID en hosts Linux y se debe observar que las direcciones IPv6 no se han asignado a los contenedores de nodos según lo esperado.

Acerca de esta tarea

Puede ver la dirección IPv6 que se ha asignado a un nodo de cuadrícula en las siguientes ubicaciones en Grid Manager:

- Seleccione **Nodes** y seleccione el nodo. A continuación, haga clic en **Mostrar más** junto a **direcciones IP** en la ficha Descripción general.

DC1-S1 (Storage Node)

Overview Hardware Network Storage Objects ILM Events

Node Information ?

Name DC1-S1
Type Storage Node
Software Version 11.1.0 (build 20180606.2152.b3bbe9d)
IP Addresses 10.96.106.102 [Show less](#) ^

Interface	IP Address
eth0	10.96.106.102
eth0	fe80::250:56ff:fea7:5c83

- Seleccione **Soporte > Herramientas > Topología de cuadrícula**. A continuación, seleccione **node > SSM > Recursos**. Si se ha asignado una dirección IPv6, se muestra debajo de la dirección IPv4 en la sección **direcciones de red**.

Si no se muestra la dirección IPv6 y el nodo está instalado en un host Linux, siga estos pasos para habilitar la compatibilidad de IPv6 en el kernel.

Pasos

1. Inicie sesión en el host como raíz o utilice una cuenta con permiso sudo.
2. Ejecute el siguiente comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

El resultado debe ser 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```



Si el resultado no es 0, consulte la documentación del sistema operativo para realizar el cambio `sysctl` configuración. A continuación, cambie el valor a 0 antes de continuar.

3. Introduzca el contenedor de nodo StorageGRID: `storagegrid node enter node-name`

4. Ejecute el siguiente comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

El resultado debería ser 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```



Si el resultado no es 1, este procedimiento no se aplica. Póngase en contacto con el soporte técnico.

5. Salga del contenedor: `exit`

```
root@DC1-S1:~ # exit
```

6. Como raíz, edite el siguiente archivo: `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Localice las dos líneas siguientes y elimine las etiquetas de comentario. A continuación, guarde y cierre el archivo.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Ejecute estos comandos para reiniciar el contenedor de StorageGRID:

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

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.