Solucionar los problemas del sistema StorageGRID

StorageGRID

NetApp
December 03, 2025

This PDF was generated from https://docs.netapp.com/es-es/storagegrid-118/troubleshoot/index.html on December 03, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Solucionar los problemas del sistema StorageGRID . . . 1
Solucionar problemas en un sistema StorageGRID: Descripción general . . . 1
Defina el problema . . . 1
Evalúe el riesgo y el impacto sobre el sistema . . . 2
Recopilación de datos . . . 2
Análisis de datos . . . 6
Lista de comprobación de información de escalado . . . 6
Solucione problemas de almacenamiento y objetos . . . 8
Confirme las ubicaciones de los datos del objeto . . . 8
Errores del almacén de objetos (volumen de almacenamiento) . . . 10
Verifique la integridad del objeto . . . 12
Solución de problemas S3 Alerta de tamaño de objeto de COLOCACIÓN demasiado grande . . . 20
Solucionar problemas de datos de objetos perdidos o faltantes . . . 22
Solucionar problemas de la alerta de almacenamiento de datos de objeto bajo . . . 35
Solucionar los problemas de las alertas de anulación de la Marca de agua de sólo lectura baja . . . 37
Solucione los problemas de la alarma de estado de almacenamiento (SST) . . . 41
Solucionar problemas de entrega de mensajes de servicios de plataforma (alarma SMTT) . . . 45
Solucionar problemas de metadatos . . . 46
Alerta de almacenamiento de metadatos baja . . . 46
Servicios: Estado - Alarma Cassandra (SVST) . . . 48
Errores de memoria agotada de Cassandra (alarma SMTT) . . . 52
Solucionar errores de certificado . . . 53
Solucione problemas del nodo de administrador y de la interfaz de usuario . . . 54
Errores de inicio de sesión . . . 54
Problemas de la interfaz de usuario . . . 58
Nodo de administración no disponible . . . 58
Solucionar problemas de red, hardware y plataforma . . . 59
Errores de «422: Entidad no procesable» . . . 59
Alerta de discrepancia de MTU de red de cuadrícula . . . 60
Alarma de error de recepción de red (NRER) . . . 61
Errores de sincronización de hora . . . 64
Linux: Problemas de conectividad de red . . . 65
Linux: El estado del nodo es «huérfano» . . . 65
Linux: Solucione problemas de compatibilidad con IPv6 . . . 66
Solucione problemas de un servidor de syslog externo . . . 68

Solucionar los problemas del sistema StorageGRID

Solucionar problemas en un sistema StorageGRID: Descripción general

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.

A menudo, puede resolver problemas por su cuenta; sin embargo, es posible que deba derivar algunos problemas al soporte técnico.

Defina el 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.

Evalúe el riesgo y el impacto sobre 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 se pueden recuperar de manera coherente.

Recopilación 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.	• Crear una línea de tiempo de cambios recientes
Revise las alertas y alarmas	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. Revise la lista de alertas y alarmas actuales para ver si StorageGRID ha identificado la causa raíz de un problema. Revise las alertas y alarmas activadas en el pasado para obtener información adicional.	• "Ver las alertas actuales y resueltas" • "Gestionar 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.	• "Supervisar eventos"

Tipo de datos que se van a recoger	Por qué recoger estos datos	Instrucciones
Identificar tendencias mediante gráficos e informes de texto	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.	• "Utilice gráficos y gráficos" • "Usar informes de texto"
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.	• Establecer 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.	• "SUPERVISE EL RENDIMIENTO DE PUT y GET"
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.	• "Revisar los mensajes de auditoría"
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.	• "Supervise las operaciones de verificación de objetos" • "Confirme las ubicaciones de los datos del objeto" • "Verifique la integridad del objeto"
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.	• "Recopilar archivos de registro y datos del sistema" • "Active manualmente un paquete AutoSupport" • "Revisar las métricas de soporte"

cree una línea de tiempo de los 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: • ¿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: • 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?

Establecer 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. Coloque el cursor sobre el gráfico para estimar cuánto almacenamiento se consume cada día Puede recopilar esta información para todo el sistema o para un centro de datos específico.
Consumo medio de metadatos	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 - metadatos de objeto, busque un punto en el que la línea sea bastante estable. Sitúe el cursor sobre el gráfico para estimar la cantidad de almacenamiento de metadatos que se consume cada día Puede recopilar esta información para todo el sistema o para un centro de datos específico.
Tasa de operaciones de S3/Swift	Operaciones por segundo	En el panel de Grid Manager, seleccione **Rendimiento** > **S3 operaciones** o **Rendimiento** > **Operaciones Swift**. Para ver las tasas y recuentos de procesamiento y recuperación de un sitio o nodo específico, seleccione **NODES** > ***site o Storage Node*** > **objetos**. Coloque el cursor sobre el gráfico de ingesta y recuperación para S3 o Swift.

Propiedad	Valor	Cómo obtener
Han fallado las operaciones de S3/Swift	Operaciones	Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. En la pestaña Overview de la sección API Operations, vea el valor de las operaciones de S3 - Failed o Swift - Failed.
Tasa de evaluación de ILM	Objetos por segundo	En la página Nodes, seleccione ***grid*** > **ILM**. En el gráfico de la cola de ILM, busque un período donde la línea sea bastante estable. Coloque el cursor sobre el gráfico para estimar un valor de línea base para **Tasa de evaluación** para su sistema.
Tasa de análisis de ILM	Objetos por segundo	Seleccione **NODES** > ***grid*** > **ILM**. En el gráfico de la cola de ILM, busque un período donde la línea sea bastante estable. Coloque el cursor sobre el gráfico para estimar un valor de línea base para **Tasa de exploración** para su sistema.
Objetos en cola de operaciones del cliente	Objetos por segundo	Seleccione **NODES** > ***grid*** > **ILM**. En el gráfico de la cola de ILM, busque un período donde la línea sea bastante estable. Coloque el cursor sobre el gráfico para estimar un valor de línea base para **Objetos en cola (de operaciones del cliente)** para su sistema.
Latencia media de consultas	Milisegundos	Seleccione **NODES** > ***Storage Node*** > **Objects**. En la tabla consultas, vea el valor de latencia media.

Análisis de 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	¿Cuáles son los síntomas del problema? ¿Cuándo comenzó el problema? ¿Ocurre de manera sistemática o intermitente? Si es intermitente, ¿qué veces ha ocurrido? Defina el problema
	Evaluación del impacto	¿Cuál es la gravedad del problema? ¿Cómo afecta a la aplicación cliente? • ¿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	En la parte superior de Grid Manager, seleccione el icono de ayuda y seleccione **Acerca de** para ver la versión de StorageGRID.
	Personalización	Resuma cómo se configura el sistema StorageGRID. Por ejemplo, enumere lo siguiente: • ¿El grid utiliza compresión de almacenamiento, cifrado de almacenamiento o cumplimiento de normativas? • ¿Hace ILM objetos replicados o con código de borrado? ¿Garantiza ILM la redundancia de sitios? ¿Las reglas de ILM usan los comportamientos de ingesta de registro equilibrado, estricto o doble?
	Registrar archivos y datos del sistema	Recopile archivos de registro y datos del sistema para su sistema. Seleccione **SUPPORT** > **Tools** > **Logs**. Es posible recopilar registros de toda la cuadrícula o de los nodos seleccionados. 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). "Recopilar archivos de registro y datos del sistema"

✔	Elemento	Notas
	Información de línea de base	Recopile información de la línea de base sobre las operaciones de ingesta, las operaciones de recuperación y el consumo de almacenamiento. Establecer líneas base
	Cronología de los cambios recientes	Crear una línea de tiempo que resume los cambios recientes realizados en el sistema o en su entorno. Crear una línea de tiempo de cambios recientes
	Historia de los esfuerzos para diagnosticar el problema	Si ha tomado medidas para diagnosticar o solucionar el problema por su cuenta, asegúrese de registrar los pasos que ha realizado y el resultado.

Solucione problemas de almacenamiento y objetos

Confirme las ubicaciones de los datos del objeto

Dependiendo del problema, es posible que desee hacerlo "confirme dónde se almacenan los datos de objetos". 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.

Antes de empezar

- 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.
  - **S3 cubo y clave de objeto**: Cuando se ingiere un objeto a través del "Interfaz de S3", la aplicación cliente utiliza una combinación de cubo y clave de objeto para almacenar e identificar el objeto.
  - **Swift contenedor y nombre de objeto**: Cuando se ingiere un objeto a través del "Interfaz Swift", la aplicación cliente utiliza una combinación de contenedor y nombre de objeto 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.

3. Si desea buscar una versión específica del objeto, escriba el ID de versión (opcional).

4. Seleccione **Buscar**.

   La "resultados de consulta de metadatos de objetos" aparecerá. Esta página incluye los siguientes tipos de información:

   - Metadatos del sistema, incluidos el ID de objeto (UUID), el ID de versión (opcional), el nombre del objeto, el nombre del contenedor, el nombre o el ID de la cuenta de inquilino, el tamaño lógico del objeto, la fecha y la hora en que se creó el objeto por primera vez, y la fecha y la 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": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


Errores del almacén de objetos (volumen de almacenamiento)

El almacenamiento subyacente en un nodo de almacenamiento se divide en almacenes de objetos. 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
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

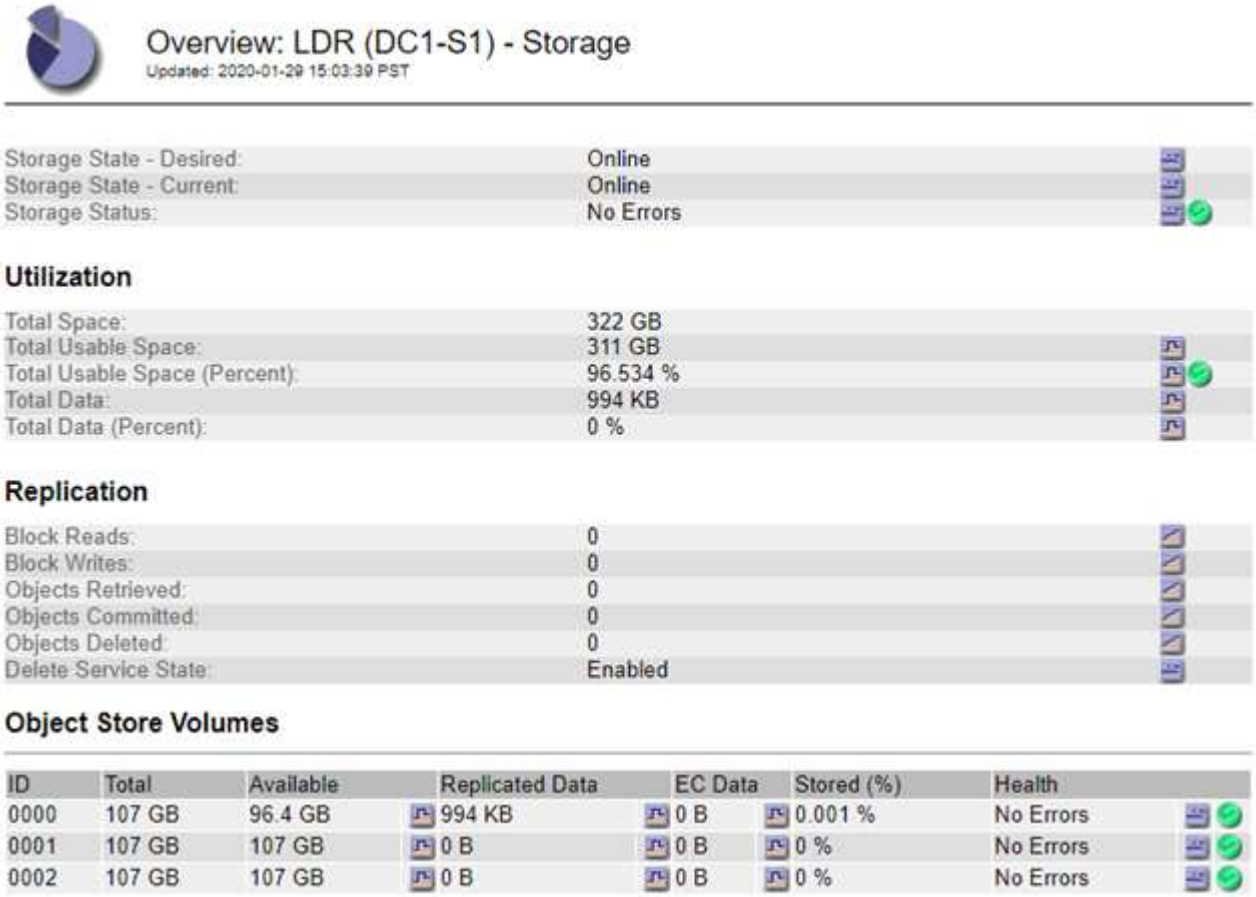
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	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
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Para ver más "Detalles de cada nodo de almacenamiento", siga estos pasos:

1. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
2. Seleccione ***site*** > ***Storage Node*** > **LDR** > **Storage** > **Overview** > **Main**.



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 pestaña **Configuración** y. "Coloque el nodo de almacenamiento en un estado de solo lectura" De modo que el sistema StorageGRID puede utilizarlo para la recuperación de datos mientras se prepara para una recuperación completa del servidor.

Verifique 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.

Existen dos procesos de verificación: Verificación de fondo y verificación de la existencia de objetos (antes denominada 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 comprobación de la existencia de objetos para verificar más rápidamente la existencia (aunque no la corrección) de objetos.

¿Qué es la verificación en segundo plano?

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 se coloca una nueva copia no dañada para cumplir las políticas de ILM activas. 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, 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. La verificación en segundo plano no se puede detener. 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 corrupto que no puede corregir automáticamente (porque la corrupción impide que el objeto sea identificado), se activa la alerta **Objeto corrupto no identificado detectado**.

Si la verificación de fondo no puede reemplazar un objeto dañado porque no puede localizar otra copia, se activa la alerta **Objetos perdidos**.

Cambie 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.

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".

Acerca de esta tarea

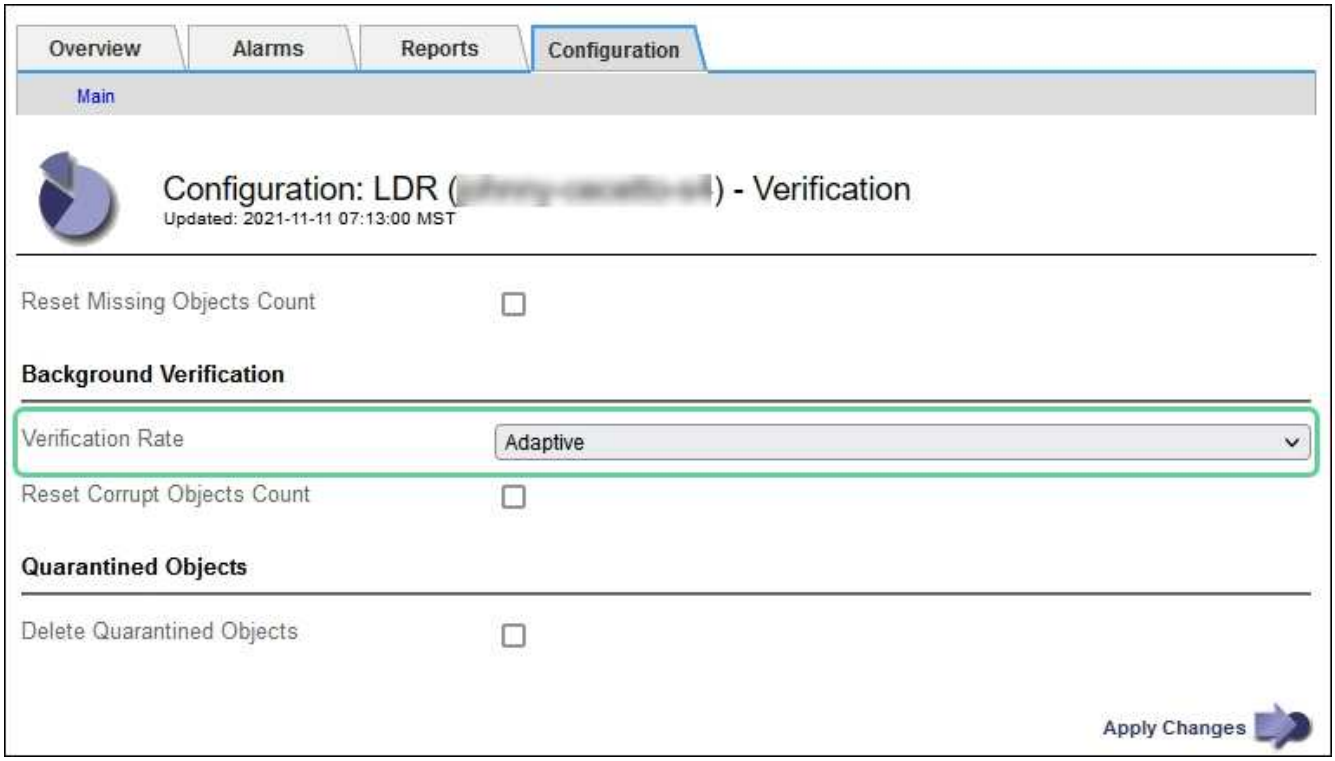
Es posible cambiar la tasa de verificación para la verificación en segundo plano en un nodo de almacenamiento:

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

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

Pasos

1. Seleccione **SUPPORT** > **Tools** > **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**.



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

6. Haga clic en **aplicar cambios**.
7. 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 se puede realizar en cualquier parte del sistema de StorageGRID que cumpla las políticas de gestión de la vida útil de la información activas.
- Si el identificador de objeto no se puede extraer (porque se ha dañado), la métrica **Objetos corruptos no identificados** aumenta y se activa la alerta **Objeto corrupto no identificado detectado**.

c. Si se encuentran datos de objeto replicado dañados, póngase en contacto con el soporte técnico para determinar la causa raíz de los daños.

8. 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 **SUPPORT** > **Tools** > **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).

9. Una vez que el sistema StorageGRID restaura automáticamente los objetos dañados, restablece el número de objetos dañados.
   a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
   b. Seleccione ***Storage Node*** > **LDR** > **Verification** > **Configuration**.
   c. Seleccione **Restablecer recuento de objetos dañados**.
   d. Haga clic en **aplicar cambios**.
10. 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.

a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
b. Seleccione ***Storage Node*** > **LDR** > **Verification** > **Configuration**.
c. Seleccione **Eliminar objetos en cuarentena**.
d. Seleccione **aplicar cambios**.

¿Qué es la comprobación de la existencia de objetos?

La comprobación de existencia de objetos verifica si todas las copias replicadas esperadas de objetos y fragmentos codificados con borrado existen en un nodo de almacenamiento. La comprobación de la existencia de objetos no comprueba los datos del objeto en sí (la verificación en segundo plano lo hace); en su lugar, proporciona una forma de verificar la integridad de los dispositivos de almacenamiento, especialmente si un problema de hardware reciente podría haber afectado a la integridad de los datos.

A diferencia de la verificación en segundo plano, que se produce automáticamente, debe iniciar manualmente un trabajo de comprobación de la existencia de objetos.

La comprobación de la existencia de objetos lee los metadatos de cada objeto almacenado en StorageGRID y verifica la existencia tanto de copias de objetos replicadas como de fragmentos de objetos con código de borrado. Los datos que faltan se tratan de la siguiente manera:

- **Copias replicadas**: Si falta una copia de los datos del objeto replicado, StorageGRID intenta automáticamente reemplazar la copia de una copia almacenada en otra parte del sistema. El nodo de almacenamiento ejecuta una copia existente a través de una evaluación de ILM, la cual determina que ya no se cumple la política actual de ILM para este objeto porque falta otra copia. Se genera y se coloca una nueva copia para satisfacer las políticas de ILM activas del sistema. Es posible que esta nueva copia no se coloque en la misma ubicación en la que se almacenó la copia que falta.
- **Fragmentos 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), ILM intenta encontrar otra copia del objeto que puede usar para generar un nuevo fragmento de código de borrado.

Ejecute la comprobación de existencia de objetos

Cree y ejecute un trabajo de comprobación de existencia de objetos a la vez. Cuando crea un trabajo, debe seleccionar los nodos de almacenamiento y los volúmenes que desea verificar. También selecciona la consistencia para el trabajo.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de mantenimiento o acceso raíz".
- Se aseguró de que los nodos de almacenamiento que desee comprobar estén en línea. Seleccione **NODES** para ver la tabla de nodos. Asegúrese de que no aparezca ningún icono de alerta junto al nombre del nodo para los nodos que desea comprobar.
- Se ha asegurado de que los siguientes procedimientos **no** se ejecutan en los nodos que desea comprobar:
  - La ampliación de grid para añadir un nodo de almacenamiento
  - Retirada del nodo de almacenamiento
  - Recuperación de un volumen de almacenamiento con fallos
  - Recuperación de un nodo de almacenamiento con una unidad del sistema con errores
  - Reequilibrio de EC
  - Clon del nodo del dispositivo

La comprobación de la existencia de objetos no proporciona información útil mientras estos procedimientos están en curso.

Acerca de esta tarea

Una tarea de comprobación de existencia de objetos puede tardar días o semanas en completarse, en función de la cantidad de objetos del grid, los nodos de almacenamiento y los volúmenes seleccionados y la coherencia seleccionada. Puede ejecutar solo un trabajo a la vez, pero puede seleccionar varios nodos y volúmenes de almacenamiento al mismo tiempo.

Pasos

1. Seleccione **MANTENIMIENTO** > **tareas** > **verificación de existencia de objeto**.
2. Seleccione **Crear trabajo**. Aparece el asistente Crear un trabajo de comprobación de existencia de objeto.

3. Seleccione los nodos que contienen los volúmenes que desea verificar. Para seleccionar todos los nodos en línea, seleccione la casilla de verificación **Nombre de nodo** en el encabezado de columna.

   Puede buscar por nombre de nodo o sitio.

   No puede seleccionar nodos que no estén conectados a la cuadrícula.

4. Seleccione **continuar**.
5. Seleccione uno o varios volúmenes para cada nodo de la lista. Es posible buscar volúmenes con el número de volumen de almacenamiento o el nombre del nodo.

   Para seleccionar todos los volúmenes para cada nodo seleccionado, seleccione la casilla de verificación **Volumen de almacenamiento** en el encabezado de columna.

6. Seleccione **continuar**.
7. Seleccione la consistencia del trabajo.

   La consistencia determina cuántas copias de metadatos de objetos se utilizan para la comprobación de existencia del objeto.

   - * Strong-site*: Dos copias de metadatos en un solo sitio.
   - **Strong-global**: Dos copias de metadatos en cada sitio.
   - **Todo** (predeterminado): Las tres copias de metadatos en cada sitio.

     Para obtener más información sobre la consistencia, consulte las descripciones en el asistente.

8. Seleccione **continuar**.
9. Revise y verifique sus selecciones. Puede seleccionar **anterior** para ir a un paso anterior del asistente para actualizar las selecciones.

   Se genera un trabajo de comprobación de existencia de objeto y se ejecuta hasta que se produce una de las siguientes acciones:

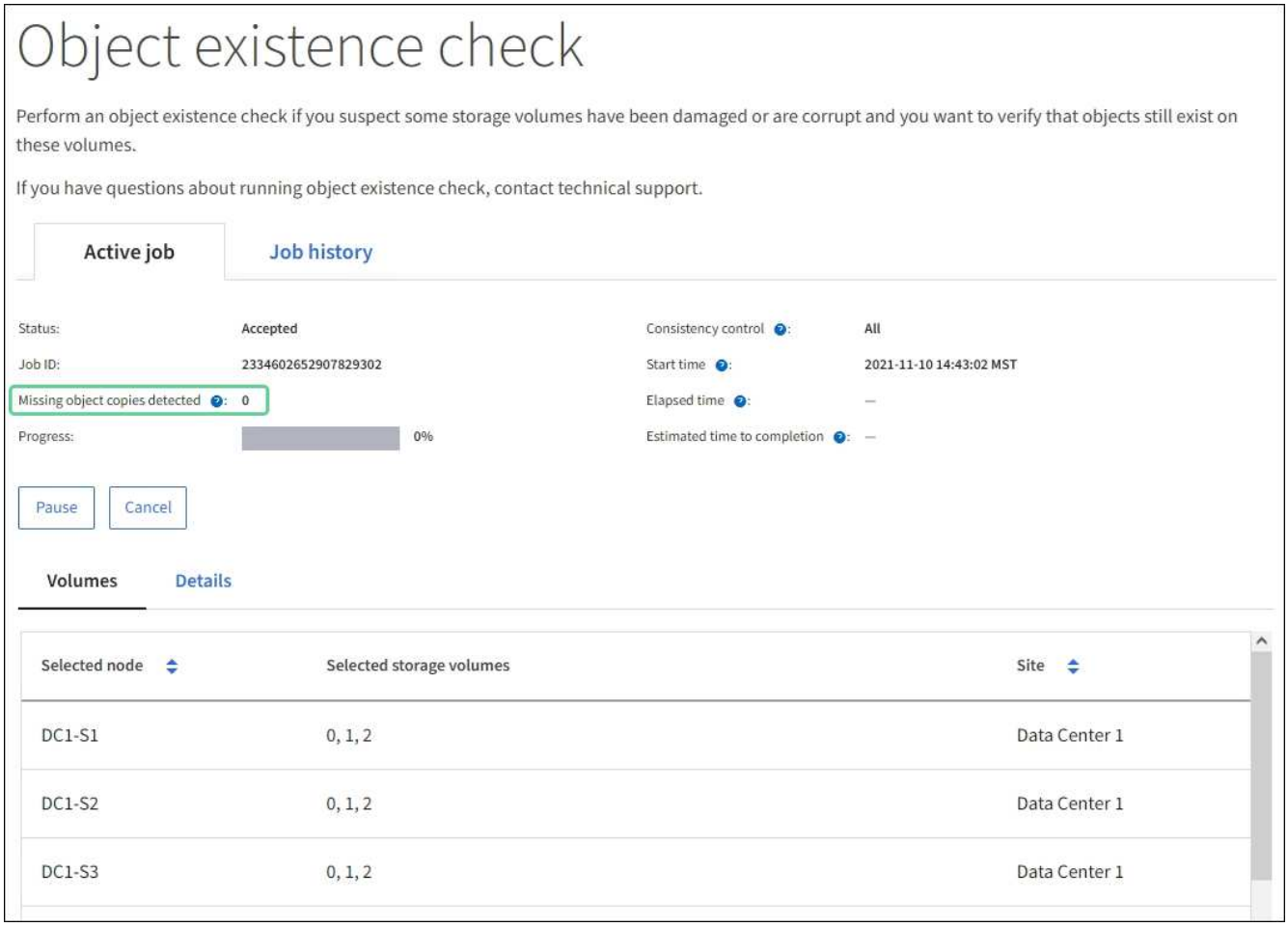
   - El trabajo finaliza.
   - El trabajo se pone en pausa o se cancela. Puede reanudar un trabajo que haya pausado, pero no puede reanudar un trabajo que haya cancelado.
   - El trabajo se cala. Se activa la alerta **comprobación de existencia de objeto ha calado**. Siga las acciones correctivas especificadas para la alerta.
   - El trabajo da error. Se activa la alerta * error de comprobación de existencia de objeto*. Siga las acciones correctivas especificadas para la alerta.
   - Aparece un mensaje que indica que el servicio no está disponible o que se ha producido un error interno del servidor. Después de un minuto, actualice la página para continuar supervisando el trabajo.

   > Según sea necesario, puede salir de la página de comprobación existencia de objetos y volver para continuar supervisando el trabajo.

10. A medida que se ejecuta el trabajo, consulte la ficha **trabajo activo** y anote el valor de las copias de objeto que faltan detectadas.

    Este valor representa el número total de copias que faltan de los objetos replicados y los objetos codificados de borrado con uno o más fragmentos que faltan.

Si el número de copias de objeto que faltan detectadas es mayor que 100, puede que haya un problema con el almacenamiento del nodo de almacenamiento.



11. Una vez completado el trabajo, realice las acciones necesarias adicionales:
    - Si las copias de objeto que faltan detectadas son cero, no se encontraron problemas. No se requiere ninguna acción.
    - Si las copias de objetos que faltan detectadas son superiores a cero y la alerta **objetos perdidos** no se ha activado, el sistema reparó todas las copias que faltan. Compruebe que se han corregido los problemas de hardware para evitar daños futuros en las copias de objetos.
    - Si las copias de objeto que faltan detectadas son superiores a cero y se ha activado la alerta **objetos perdidos**, la integridad de los datos podría verse afectada. Póngase en contacto con el soporte técnico.
    - Puede investigar las copias de objetos perdidos mediante grep para extraer los mensajes de auditoría LLST: `grep LLST audit_file_name`.

      Este procedimiento es similar al de "investigar objetos perdidos", aunque para las copias de objetos que busca `LLST` en lugar de `OLST`.

12. Si seleccionó la coherencia de sitio seguro o global fuerte para la tarea, espere aproximadamente tres semanas para mantener la coherencia de metadatos y vuelva a ejecutar el trabajo en los mismos volúmenes.

    Cuando StorageGRID tiene tiempo para lograr la consistencia de metadatos en los nodos y volúmenes incluidos en el trabajo, al volver a ejecutar el trabajo se podría eliminar por error las copias de objetos que

faltan o hacer que se comprobaran copias de objetos adicionales si se perdía.

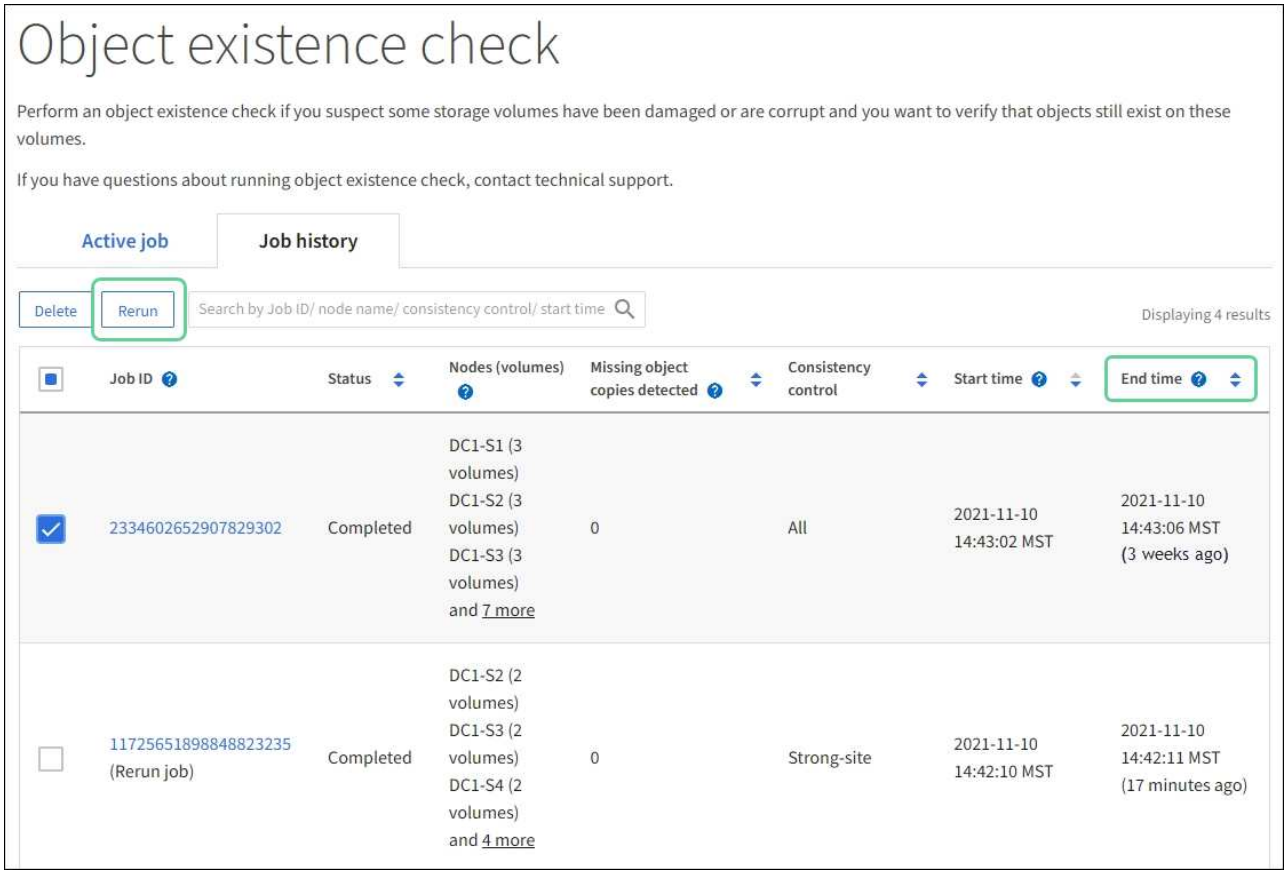
a. Seleccione **MANTENIMIENTO** > **verificación de existencia de objetos** > **Historial de trabajos**.

b. Determine qué trabajos están listos para volver a ejecutar:

   i. Observe la columna **tiempo final** para determinar qué trabajos se ejecutaron hace más de tres semanas.

   ii. En el caso de estos trabajos, analice la columna de control de coherencia para obtener un sitio seguro o un entorno global sólido.

c. Seleccione la casilla de verificación para cada trabajo que desee volver a ejecutar y, a continuación, seleccione **Volver a ejecutar**.



d. En el asistente Rerun Jobs, revise los nodos y los volúmenes seleccionados y la coherencia.

e. Cuando esté listo para volver a ejecutar los trabajos, seleccione **Rerun**.

Aparece la ficha Trabajo activo. Todos los trabajos que ha seleccionado se vuelven a ejecutar como un trabajo a una consistencia de sitio fuerte. En el campo **trabajos relacionados** de la sección Detalles se muestran los identificadores de trabajo de los trabajos originales.

Después de terminar

Si aún tiene dudas sobre la integridad de los datos, vaya a **SUPPORT** > **Tools** > **Grid topolog** > ***site*** > ***Storage Node*** > **LDR** > **Verification** > **Configuration** > **Main** y aumente la velocidad 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.

Solución de problemas S3 Alerta de tamaño de objeto de COLOCACIÓN demasiado grande

La alerta S3 PUT Object size too large se activa si un arrendatario intenta una operación PutObject que no es de varias partes que supera el límite de tamaño de S3 GB de 5 GiB.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".

Determine qué inquilinos utilizan objetos mayores de 5 GiB, para que pueda notificarlos.

Pasos

1. Vaya a **CONFIGURACIÓN** > **Monitoreo** > **Servidor de auditoría y syslog**.
2. Si las escrituras de cliente son Normal, acceda al registro de auditoría:

   a. Introduzca `ssh admin@primary_Admin_Node_IP`

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

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

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

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

   e. Cambie al directorio donde se encuentran los registros de auditoría.

   El directorio de registro de auditoría y los nodos aplicables dependen de la configuración del destino de auditoría.

Opción	Destino
Nodos locales (predeterminado)	`/var/local/log/localaudit.log`
Nodos de administración/nodos locales	• Nodos de administración (primarios y no primarios): `/var/local/audit/export/audit.log` • Todos los nodos: El `/var/local/log/localaudit.log` archivo normalmente está vacío o falta en este modo.
Servidor de syslog externo	`/var/local/log/localaudit.log`

   En función de la configuración de destino de auditoría, introduzca: `cd /var/local/log` O. `/var/local/audit/export/`

   Para obtener más información, consulte "Seleccione destinos de información de auditoría".

   f. Identifique qué inquilinos están usando objetos mayores de 5 GiB.

   i. Introduzca `zgrep SPUT * | egrep "CSIZ\(UI64\):([5-9]|[1-9][0-9]+)[0-9]{9}"`

   ii. Para cada mensaje de auditoría de los resultados, consulte `S3AI` Para determinar el ID de cuenta

de inquilino. Utilice los otros campos del mensaje para determinar la dirección IP utilizada por el cliente, el depósito y el objeto:

Codificación	Descripción
SAIP	IP de origen
S3AI	ID de inquilino
S3BK	Cucharón
S3KY	Objeto
CSIZ	Tamaño (bytes)

Ejemplo de resultados de registro de auditoría

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):804317333][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CSTR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:identity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][SBAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Si las escrituras del cliente no son normales, use el ID de inquilino de la alerta para identificar el inquilino:

   a. Vaya a **SUPPORT** > **Tools** > **Logs**. Recopile registros de la aplicación para el nodo de almacenamiento en la alerta. Especifique 15 minutos antes y después de la alerta.

   b. Extraiga el archivo y vaya a. `bycast.log`:

      `/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log`

   c. Busque en el log `method=PUT` e identificar al cliente en el `clientIP` campo.

      Ejemplo bycast.log

```
Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA 2023-01-05T18:33:41.208790| NOTICE   1404 af23cb66b7e3efa5 S3RQ: EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
```

4. Informe a los inquilinos que el tamaño máximo de PutObject es de 5 GiB y que utilicen cargas de varias partes para objetos de más de 5 GiB.
5. Ignore la alerta durante una semana si la aplicación ha cambiado.

Solucionar problemas de datos de objetos perdidos o faltantes

Solucionar problemas de datos de objetos perdidos o faltantes: Descripción general

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, la alerta **objetos perdidos** se activa de la siguiente manera:

- En el caso de las copias replicadas, si no se puede recuperar otra copia, el objeto se considera perdido y se activa la alerta.
- En el caso de las copias con código de borrado, si no se puede recuperar una copia de la ubicación esperada, el atributo Copias dañadas detectadas (ECOR) aumenta en uno antes de intentar recuperar una copia de otra ubicación. Si no se encuentra ninguna otra copia, se activa la alerta.

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. Consulte "Investigar los objetos perdidos".

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

Investigar los objetos perdidos

Cuando se activa la alerta **objetos perdidos**, debe investigar inmediatamente. Recopile información sobre los objetos afectados y póngase en contacto con el soporte técnico.

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".
- Debe tener la `Passwords.txt` archivo.

Acerca de esta tarea

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

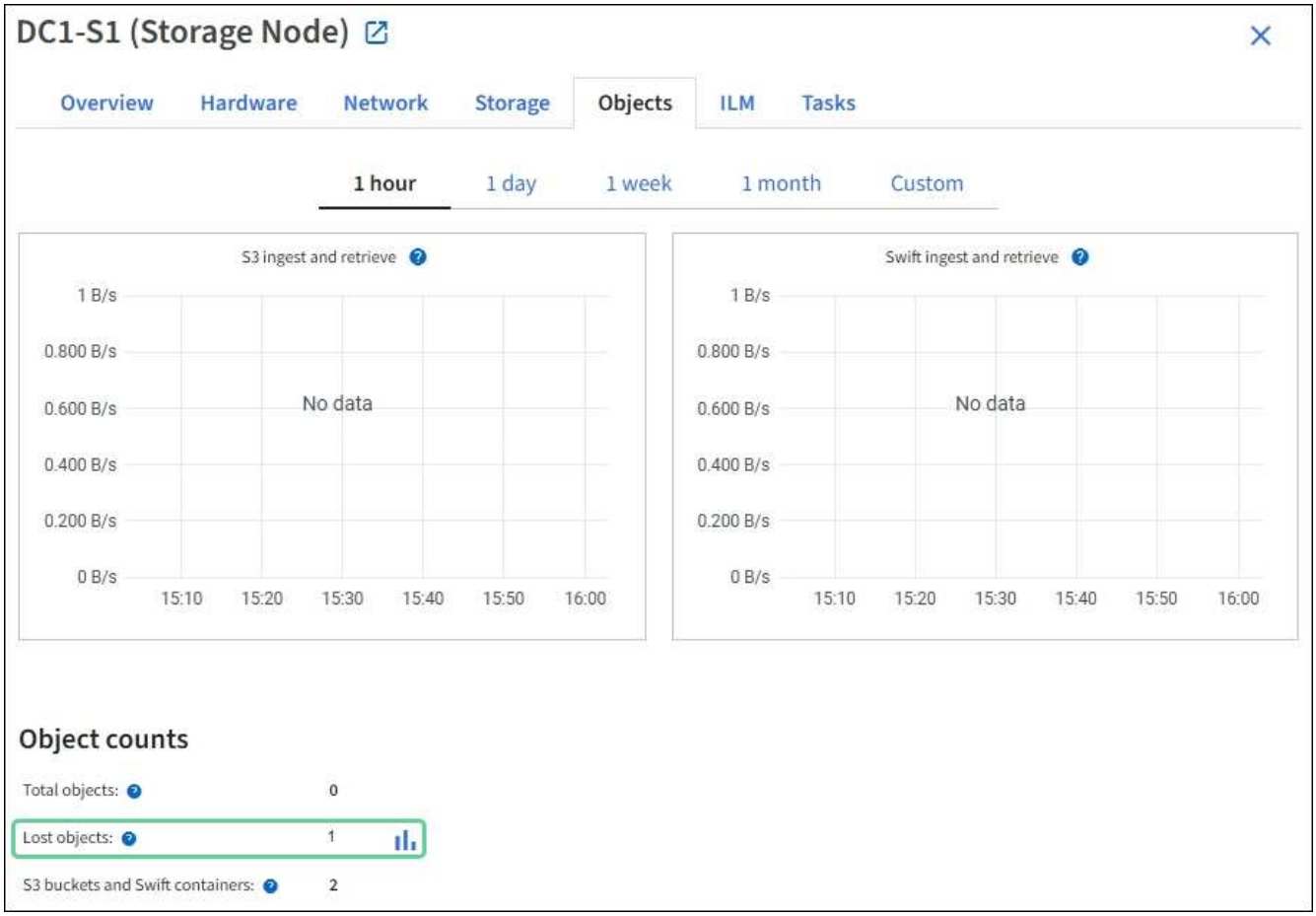
Investigar las alertas de objetos perdidos de inmediato. Es posible que deba tomar medidas para evitar la pérdida de datos adicional. En algunos casos, es posible que pueda restaurar un objeto perdido si realiza una

acción rápida.

Pasos

1. Selecciona **NODOS**.
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**:
   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.

      El directorio de registro de auditoría y los nodos aplicables dependen de la configuración del destino de auditoría.

Opción	Destino
Nodos locales (predeterminado)	`/var/local/log/localaudit.log`
Nodos de administración/nodos locales	• Nodos de administración (primarios y no primarios): `/var/local/audit/export/audit.log` • Todos los nodos: El `/var/local/log/localaudit.log` archivo normalmente está vacío o falta en este modo.
Servidor de syslog externo	`/var/local/log/localaudit.log`

En función de la configuración de destino de auditoría, introduzca: `cd /var/local/log` O. `/var/local/audit/export/`

Para obtener más información, consulte "Seleccione destinos de información de auditoría".

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. Use SSH para iniciar sesión en cualquier nodo de almacenamiento. A continuación, acceda a la consola LDR introduciendo telnet 0 1402.

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":"")	Si no se encuentra el objeto, se devuelve el mensaje "ERROR":". Si no se encuentra el objeto, puede restablecer el recuento de **objetos perdidos** para borrar la alerta. La falta de un objeto indica que el objeto se ha eliminado intencionalmente.
Ubicaciones > 0	Si hay ubicaciones enumeradas en la salida, la alerta **objetos perdidos** podría ser un falso positivo. 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. (Procedimiento para "buscando objetos potencialmente perdidos" Explica cómo usar el ID de nodo para encontrar el nodo de almacenamiento correcto.) Si los objetos existen, puede restablecer el recuento de **objetos perdidos** para borrar la alerta.
Ubicaciones = 0	Si no hay ninguna ubicación en la salida, el objeto puede faltar. Puede intentar "busque y restaure el objeto" usted mismo o puede ponerse en contacto con el soporte técnico. Es posible que el soporte técnico le solicite determinar si hay un procedimiento de recuperación del almacenamiento en curso. Consulte la información acerca de "Restaurando datos de objetos con Grid Manager" y.. "restaurar datos de objeto en un volumen de almacenamiento".

Busque y restaure objetos que se han perdido potencialmente

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.

Antes de empezar

- Tiene el UUID de cualquier objeto perdido, como se identifica en "Investigar los objetos perdidos".
- Usted tiene 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.

      El directorio de registro de auditoría y los nodos aplicables dependen de la configuración del destino de auditoría.

Opción	Destino
Nodos locales (predeterminado)	`/var/local/log/localaudit.log`
Nodos de administración/nodos locales	• Nodos de administración (primarios y no primarios): `/var/local/audit/export/audit.log` • Todos los nodos: El `/var/local/log/localaudit.log` archivo normalmente está vacío o falta en este modo.
Servidor de syslog externo	`/var/local/log/localaudit.log`

      En función de la configuración de destino de auditoría, introduzca: `cd /var/local/log` O. `/var/local/audit/export/`

      Para obtener más información, consulte "Seleccione destinos de información de auditoría".

   c. Utilice grep para extraer el "mensajes de auditoría asociados con el objeto potencialmente perdido" y envíelos 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 >
/var/local/tmp/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 /var/local/tmp/messages_about_lost_objects.txt
```

Un mensaje de auditoría LLST tiene el aspecto de 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):15815351
34379225]
[ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CLSM][ATID(UI64):70
868710831907434 09]]
```

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.

a. Busque el nodo de almacenamiento asociado a este ID de nodo LDR. En Grid Manager, seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***Data Center*** > ***Storage Node*** > **LDR**.

El identificador de nodo para el servicio LDR está en la tabla Información de Nodo. Revise la información de cada nodo de almacenamiento hasta que encuentre el que aloja esta LDR.

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'
```

> Escriba siempre la ruta de acceso del archivo de objetos entre comillas simples en comandos para escapar de caracteres especiales.

- Si no se encuentra la ruta del objeto, el objeto se pierde y no se puede restaurar mediante este procedimiento. Póngase en contacto con el soporte técnico.

- Si se encuentra la ruta del objeto, continúe con el paso siguiente. Puede intentar restaurar el objeto encontrado de nuevo en StorageGRID.

3. 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. Use SSH para iniciar sesión en cualquier nodo de almacenamiento. A continuación, acceda a la consola LDR introduciendo 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 las políticas de ILM activas, que realizan copias adicionales según se especifica en cada política.

      > 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 próximo paso.

4. 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`

5. 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. Consulte subpaso 1. b.

   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 >
      /var/local/tmp/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 /var/local/tmp/messages_about_restored_object.txt
      ```

      Un mensaje de auditoría ORLM tiene el aspecto de 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.

6. "Restablezca el recuento de objetos perdidos o faltantes" En Grid Manager.

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.

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".

Acerca de esta tarea

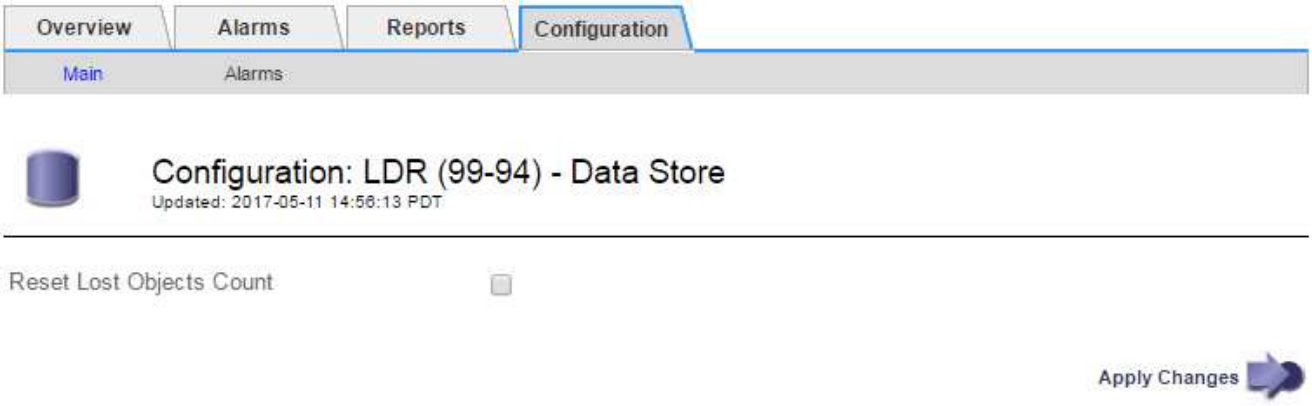
Puede restablecer el contador objetos perdidos desde cualquiera de las siguientes páginas:

- **SOPORTE** > **Herramientas** > **Topología de cuadrícula** > ***Sitio*** > ***nodo de almacenamiento*** > **LDR** > **almacén de datos** > **Descripción general** > **Principal**
- **SUPPORT** > **Herramientas** > **Topología de cuadrícula** > ***Site*** > ***Storage Node*** > **DDS** > **Data Store** > **Overview** > **Main**

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

Pasos

1. Seleccione **SUPPORT** > **Tools** > **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**.



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**.

Solucionar problemas de la alerta de almacenamiento de datos de objeto bajo

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "permisos de acceso específicos".

Acerca de esta tarea

La alerta **Low object data storage** se activa cuando la cantidad total de datos de objetos replicados y borrados en un nodo de almacenamiento cumple con 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 replicados y codificados de 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 **ALERTS** > **Current**.

   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.

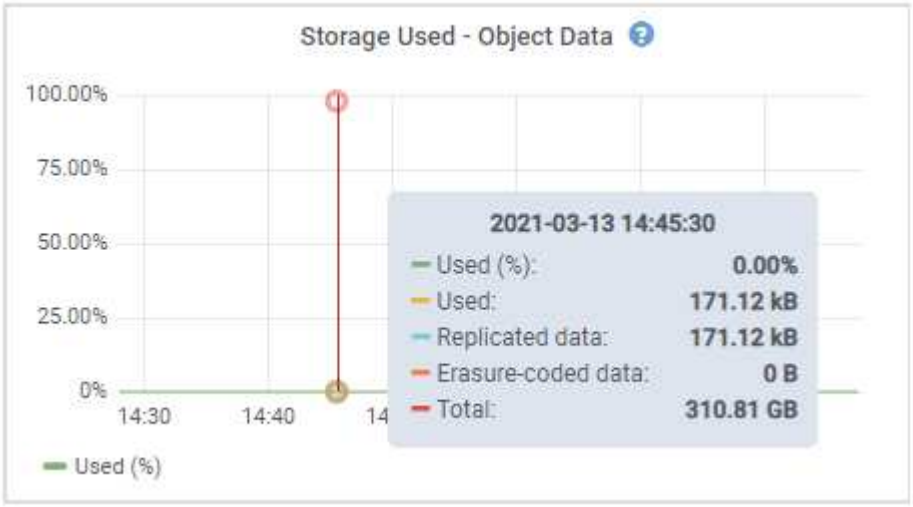
   Seleccione la alerta, no el encabezado de un grupo de alertas.

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. Coloque 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, "añadir capacidad de almacenamiento" en la cuadrícula.

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

   Para obtener más información, consulte "Gestione nodos de almacenamiento completos".

Información relacionada

"Solucionar problemas de la alarma de estado de almacenamiento (SST) (heredado)"

Solucionar los problemas de las alertas de anulación de la Marca de agua de sólo lectura baja

Si utiliza valores personalizados para las marcas de agua del volumen de almacenamiento, puede que necesite resolver la alerta **anulación de Marca de agua de sólo lectura baja**. Si es posible, debe actualizar el sistema para empezar a utilizar los valores optimizados.

En versiones anteriores, las tres "marcas de agua de volumen de almacenamiento" Eran una configuración global y no 8212; los mismos valores se aplicaban a cada volumen de almacenamiento en cada nodo de almacenamiento. A partir de StorageGRID 11.6, el software puede optimizar estas marcas de agua para cada volumen de almacenamiento en función del tamaño del nodo de almacenamiento y la capacidad relativa del volumen.

Cuando se actualiza a StorageGRID 11,6 o superior, las marcas de agua optimizadas de solo lectura y de lectura y escritura se aplican automáticamente a todos los volúmenes de almacenamiento, a menos que se cumpla alguna de las siguientes situaciones:

- El sistema está cerca de su capacidad y no podría aceptar datos nuevos si se aplicaran marcas de agua optimizadas. En este caso, StorageGRID no cambiará la configuración de la Marca de agua.
- Anteriormente, se estableció cualquiera de las marcas de agua del volumen de almacenamiento en un valor personalizado. StorageGRID no anulará la configuración personalizada de la Marca de agua con valores optimizados. Sin embargo, StorageGRID puede activar la alerta **anulación de Marca de agua de sólo lectura baja** si su valor personalizado para la Marca de agua de sólo lectura suave de volumen de almacenamiento es demasiado pequeño.

Comprenda la alerta

Si utiliza valores personalizados para las marcas de agua del volumen de almacenamiento, puede activarse la alerta **anulación de Marca de agua de sólo lectura baja** para uno o más nodos de almacenamiento.

Cada instancia de la alerta indica que el valor personalizado de **Marca de agua de sólo lectura suave de volumen de almacenamiento** es menor que el valor mínimo optimizado para ese nodo de almacenamiento. Si continúa utilizando la configuración personalizada, es posible que el nodo de almacenamiento se ejecute con un espacio mínimo antes de que pueda realizar una transición segura al estado de solo lectura. Es posible que algunos volúmenes de almacenamiento no se puedan acceder a ellos (se desmontan automáticamente) cuando el nodo alcanza la capacidad.

Por ejemplo, supongamos que previamente ha establecido la Marca **Marca de agua blanda de sólo lectura de volumen de almacenamiento** en 5 GB. Ahora supongamos que StorageGRID ha calculado los siguientes valores optimizados para los cuatro volúmenes de almacenamiento en el nodo De almacenamiento A:

Volumen 0	12 GB
Volumen 1	12 GB
Volumen 2	11 GB
Volumen 3	15 GB

La alerta **Baja de sólo lectura de anulación de Marca de agua** se activa para el nodo De almacenamiento A porque su Marca de agua personalizada (5 GB) es menor que el valor mínimo optimizado para todos los volúmenes de ese nodo (11 GB). Si continúa usando la configuración personalizada, el nodo podría ejecutarse con un nivel mínimo de espacio antes de que pueda realizar la transición de forma segura al estado de solo lectura.

Resolver la alerta

Siga estos pasos si se ha activado una o más alertas **Baja de sustitución de Marca de agua de sólo lectura**. También puede utilizar estas instrucciones si actualmente utiliza la configuración personalizada de Marca de agua y desea comenzar a utilizar la configuración optimizada incluso si no se ha activado ninguna alerta.

Antes de empezar

- Ha completado la actualización a StorageGRID 11,6 o superior.
- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Usted tiene la "Permiso de acceso raíz".

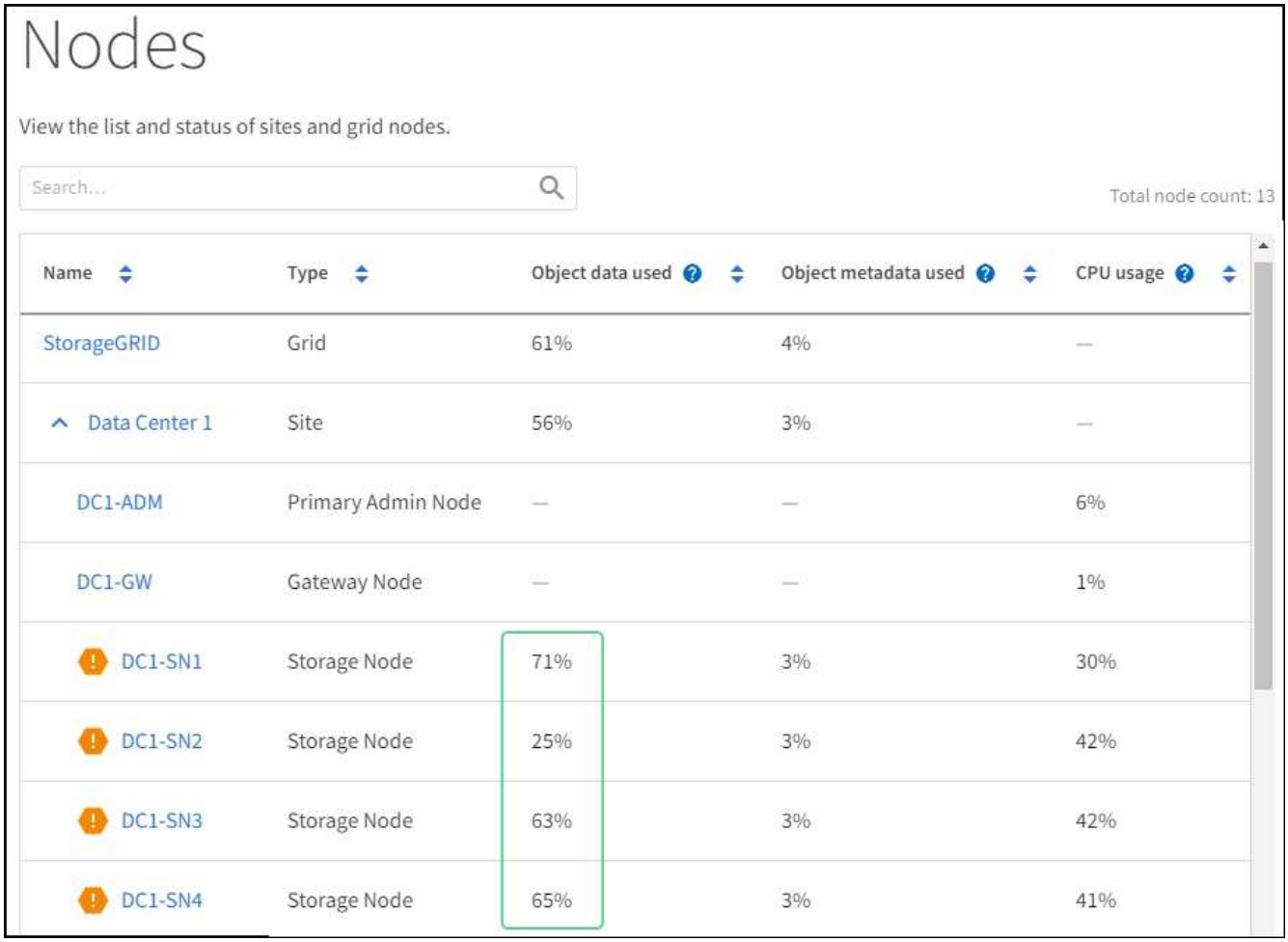
Acerca de esta tarea

Puede resolver la alerta **anulación de Marca de agua de sólo lectura baja** actualizando la configuración de Marca de agua personalizada a las nuevas anulaciones de Marca de agua. Sin embargo, si uno o varios nodos de almacenamiento están cerca de su totalidad o tiene requisitos especiales de gestión del ciclo de vida de la información, primero debe ver las marcas de agua de almacenamiento optimizadas y determinar si es seguro utilizarlas.

Evalúe el uso de datos de objetos en todo el grid

Pasos

1. Selecciona **NODOS**.
2. Para cada sitio de la cuadrícula, expanda la lista de nodos.
3. Revise los valores porcentuales que se muestran en la columna **datos de objeto utilizados** para cada nodo de almacenamiento de cada sitio.



4. Siga el paso apropiado:
   a. Si ninguno de los nodos de almacenamiento está cerca de lleno (por ejemplo, todos los valores de **datos de objeto utilizados** son inferiores al 80%), puede empezar a utilizar la configuración de anulación. Vaya a. Utilice marcas de agua optimizadas.
   b. Si las reglas de ILM utilizan un comportamiento de ingesta estricto o si los pools de almacenamiento específicos están casi completos, siga los pasos de Vea las marcas de agua de almacenamiento optimizadas y.. Determine si puede utilizar marcas de agua optimizadas.

Ver marcas de agua de almacenamiento optimizadas

StorageGRID utiliza dos métricas Prometheus para mostrar los valores optimizados que ha calculado para la Marca de agua * de sólo lectura suave de volumen de almacenamiento*. Puede ver los valores mínimos y máximos optimizados para cada nodo de almacenamiento en la cuadrícula.

Pasos

1. Seleccione **SUPPORT** > **Tools** > **Metrics**.
2. En la sección Prometheus, seleccione el enlace para acceder a la interfaz de usuario de Prometheus.
3. Para ver la Marca de agua blanda de sólo lectura recomendada, introduzca la siguiente métrica Prometheus y seleccione **Ejecutar**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   La última columna muestra el valor optimizado mínimo de la Marca de agua de solo lectura suave para todos los volúmenes de almacenamiento de cada nodo de almacenamiento. Si este valor es mayor que el valor personalizado para **Marca de agua blanda de sólo lectura de volumen de almacenamiento**, se activa la alerta **anulación de Marca de agua de sólo lectura baja** para el nodo de almacenamiento.

4. Para ver la Marca de agua blanda de sólo lectura recomendada, introduzca la siguiente métrica Prometheus y seleccione **Ejecutar**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   La última columna muestra el valor optimizado máximo de la Marca de agua de solo lectura suave para todos los volúmenes de almacenamiento de cada nodo de almacenamiento.

5. Observe el valor optimizado máximo para cada nodo de almacenamiento.

Determine si puede utilizar marcas de agua optimizadas

Pasos

1. Selecciona **NODOS**.
2. Repita estos pasos para cada nodo de almacenamiento en línea:
   a. Seleccione ***Storage Node*** > **Storage**.
   b. Desplácese hasta la tabla almacenes de objetos.
   c. Compare el valor **disponible** de cada almacén de objetos (volumen) con la Marca de agua optimizada máxima que anotó para ese nodo de almacenamiento.
3. Si al menos un volumen de cada nodo de almacenamiento en línea tiene más espacio disponible que la Marca de agua máxima optimizada para ese nodo, vaya a. Utilice marcas de agua optimizadas para empezar a utilizar las marcas de agua optimizadas.

   De lo contrario, amplíe la cuadrícula lo antes posible. Uno de los dos "añadir volúmenes de almacenamiento" en un nodo existente o. "Añada nuevos nodos de almacenamiento". A continuación, vaya a. Utilice marcas de agua optimizadas para actualizar la configuración de la marca de agua.

4. Si debe continuar utilizando valores personalizados para las marcas de agua del volumen de almacenamiento, "silencio" o. "desactivar" La alerta **Baja de sólo lectura de la Marca de agua anulando**.

Los mismos valores de Marca de agua personalizados se aplican a cada volumen de almacenamiento de cada nodo de almacenamiento. Si se utilizan valores más pequeños de lo recomendado para las marcas de agua del volumen de almacenamiento, es posible que algunos volúmenes de almacenamiento se vuelvan inaccesibles (se desmontan automáticamente) cuando el nodo alcanza la capacidad.

Utilice marcas de agua optimizadas

Pasos

1. Vaya a **SUPPORT** > **Other** > **Marcas de agua de almacenamiento**.
2. Seleccione la casilla de verificación **Usar valores optimizados**.
3. Seleccione **Guardar**.

La configuración de Marca de agua del volumen de almacenamiento optimizada ahora está en vigor para cada volumen de almacenamiento, según el tamaño del nodo de almacenamiento y la capacidad relativa del volumen.

Solucione los 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.

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "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** > **sistema** > **opciones de almacenamiento**).

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

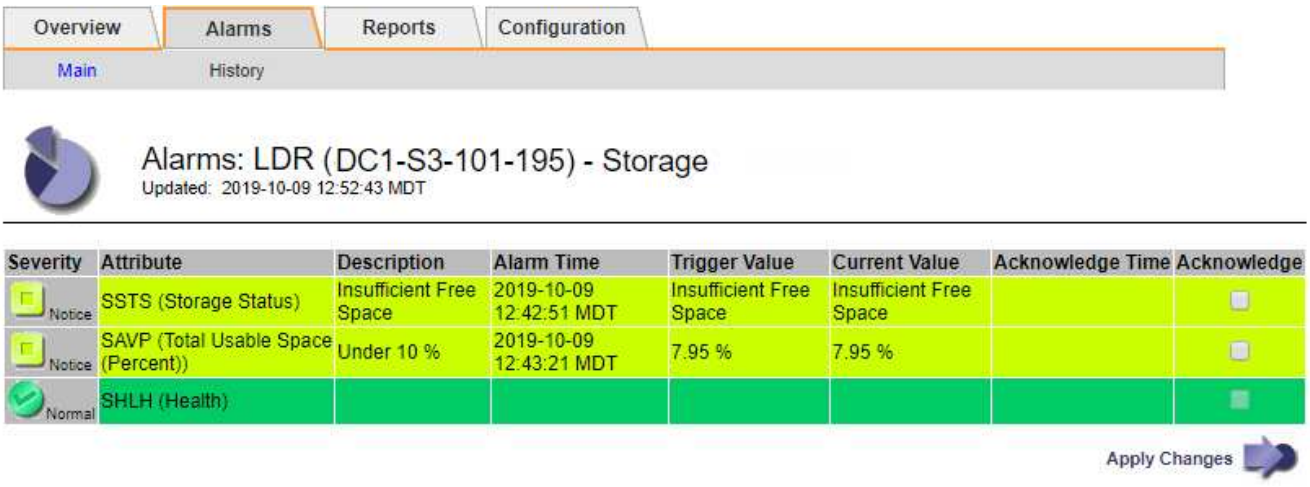
Por ejemplo, supongamos que la Marca de agua de sólo lectura suave del volumen de almacenamiento se establece en 10 GB, que es su valor predeterminado. La alarma SSTS se activa si queda menos de 10 GB de espacio utilizable en cada volumen de almacenamiento del nodo de almacenamiento. Si alguno de los 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 **SUPPORT** > **Alarms (Legacy)** > **Current Alarms**.
2. En la columna Servicio, seleccione el centro de datos, el nodo y el servicio asociados a la alarma SSTS.

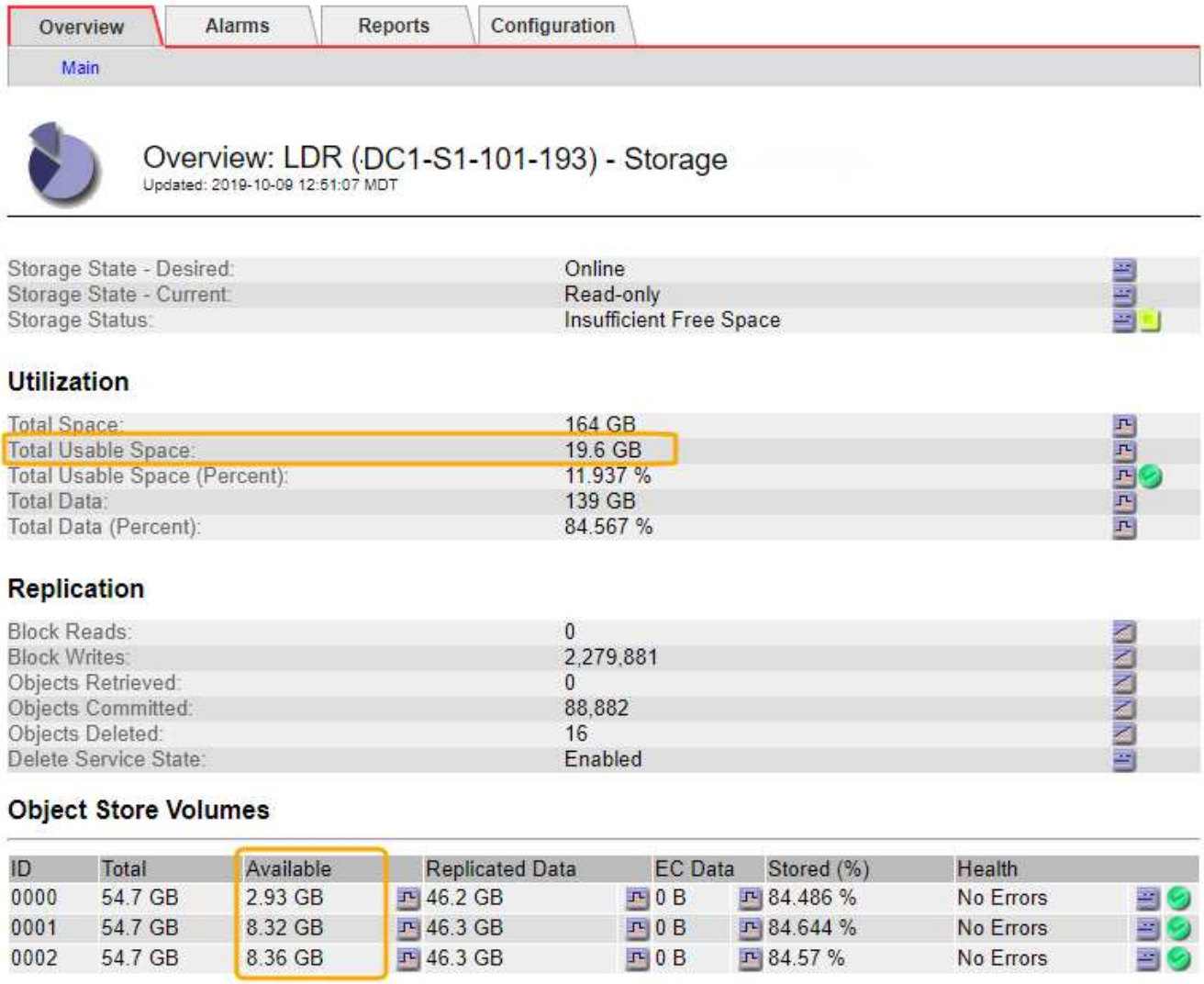
   Aparece la página Topología de cuadrícula. La ficha Alarmas muestra las alarmas activas del nodo y el servicio que ha seleccionado.



   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.

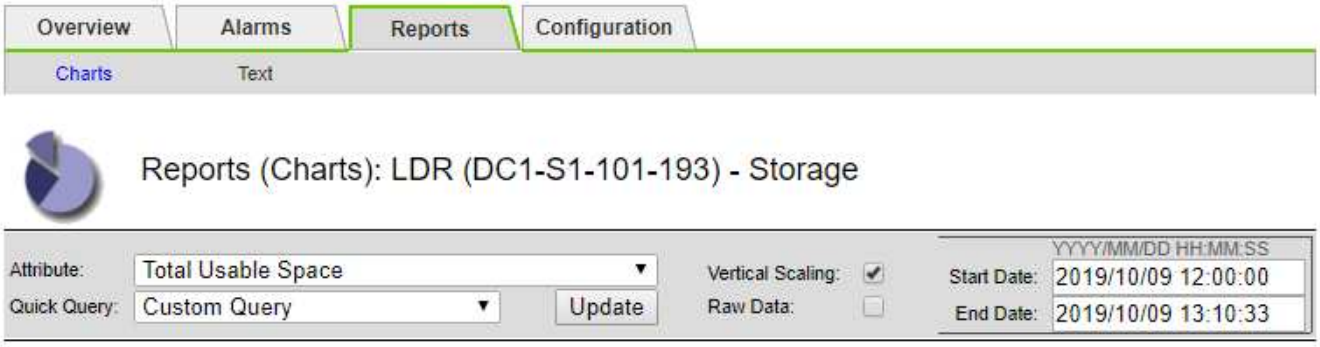
3. Para determinar cuánto espacio útil está realmente disponible, seleccione **LDR** > **almacenamiento** > **Descripción general** y busque el atributo espacio útil total (STS).

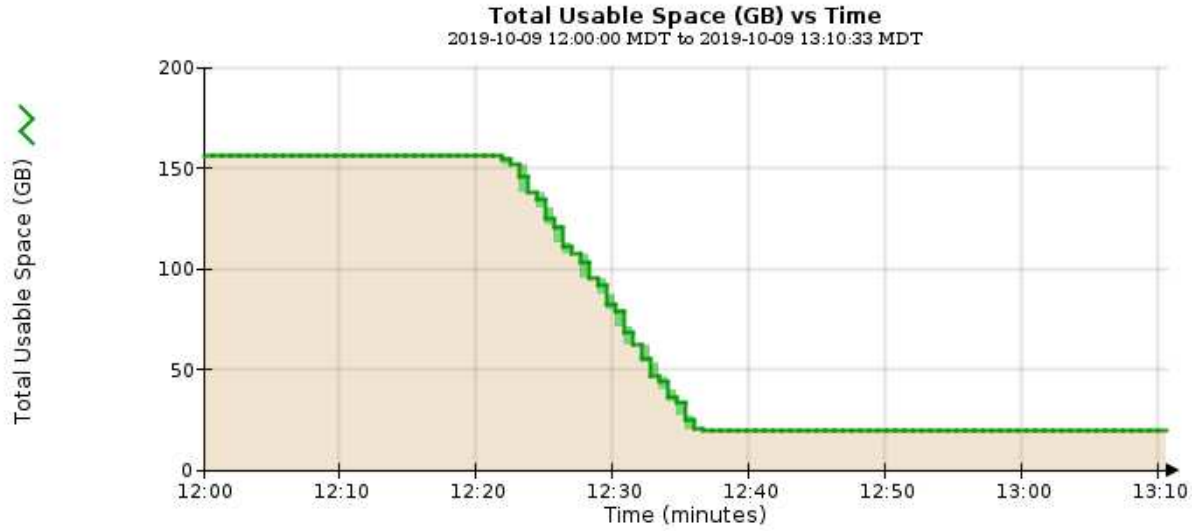


En este ejemplo, solo quedan disponibles 19.6 GB del espacio de 164 GB en este nodo de almacenamiento. Tenga en cuenta que el valor total es la suma de los valores **disponible** para los tres volúmenes de almacén de objetos. Se activó la alarma DE SSTS porque cada uno de los tres volúmenes de almacenamiento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

4. 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.

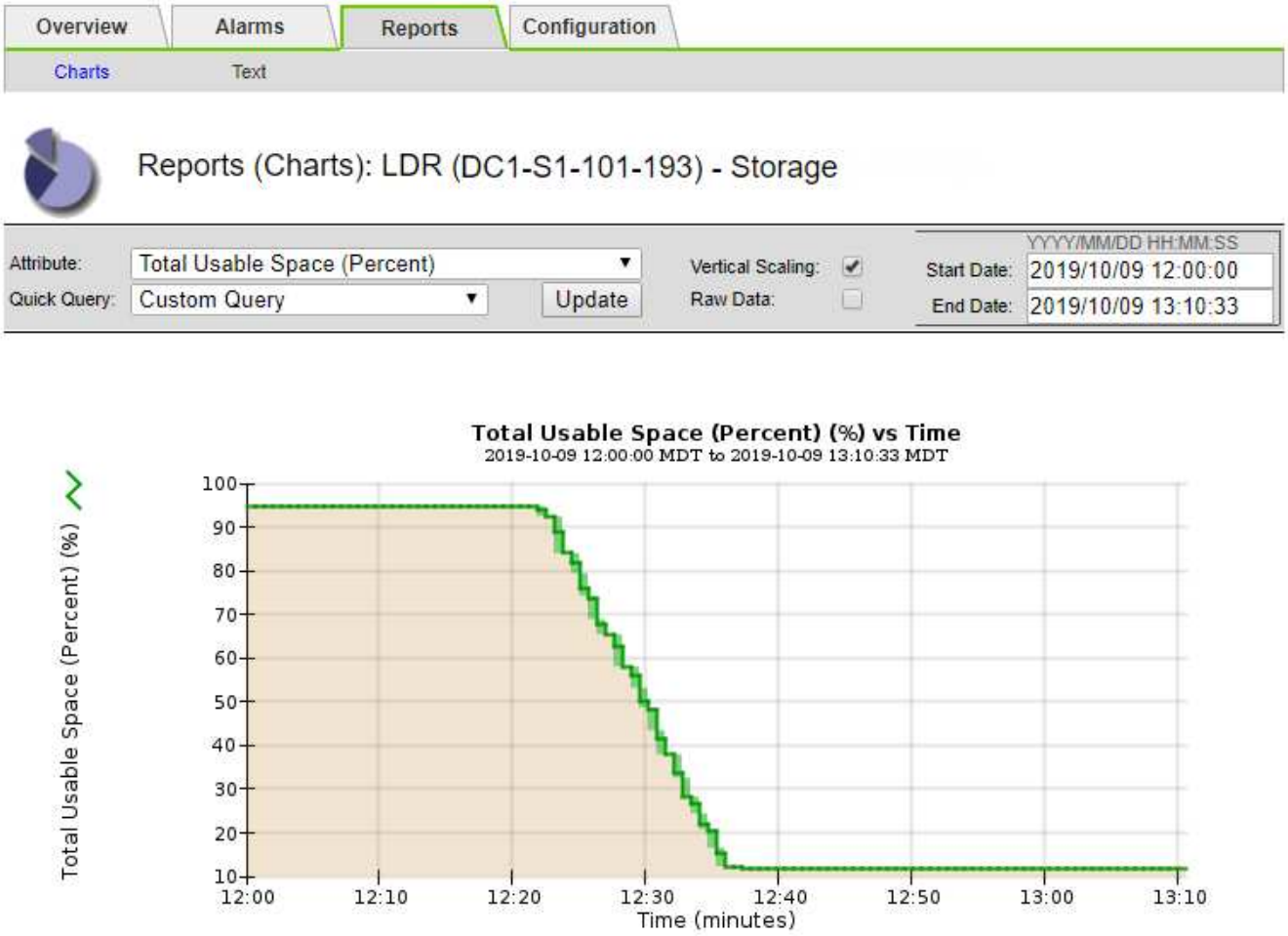
   En este ejemplo, el espacio útil total cayó de aproximadamente 155 GB a 12:00 a 20 GB a 12:35, lo que corresponde al tiempo en que se activó la alarma DE SST.





5. 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.



6. Según sea necesario, "añadir capacidad de almacenamiento".

   Consulte también "Gestione nodos de almacenamiento completos".

Solucionar problemas de entrega de mensajes de servicios de plataforma (alarma SMTT)

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

Acerca de esta tarea

Por ejemplo, una carga de varias partes de S3 puede realizarse correctamente aunque el mensaje de replicación o notificación asociado no se pueda entregar al punto final 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.

Los mensajes de eventos también aparecen en la `/var/local/log/bycast-err.log` archivo de registro. Consulte "Referencia de archivos de registro".

Para obtener más información, consulte "Solucione problemas de servicios de plataforma". Puede que necesite hacerlo "Acceda al inquilino del 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. Seleccione **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.

Solucionar problemas de metadatos

Puede realizar varias tareas para determinar el origen de los problemas de metadatos.

Alerta de almacenamiento de metadatos baja

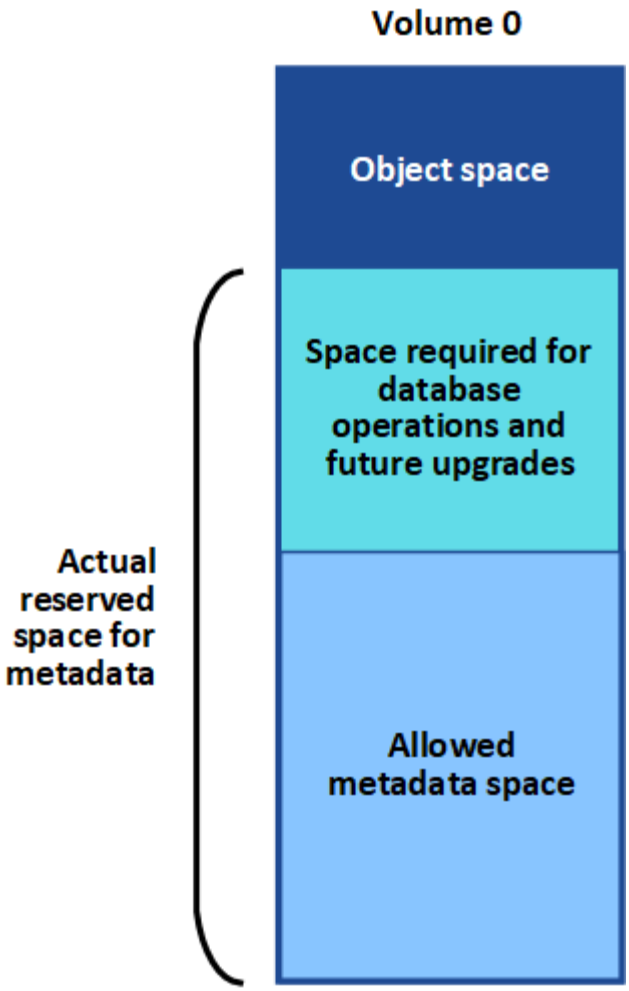
Si se activa la alerta **almacenamiento de metadatos bajo**, debe agregar nuevos nodos de almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web 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 objetos consumen más del 100% del espacio permitido para los metadatos, las operaciones de la base de datos no se podrán ejecutar de manera eficiente y se producirán errores.

Puede hacerlo "Supervise la capacidad de metadatos de los objetos para cada nodo de almacenamiento" para ayudarle a anticiparse a los errores y corregirlos antes de que ocurran.

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

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_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..
- **Major**: Los metadatos de objetos utilizan un 90% o más del espacio de metadatos permitido. Debe añadir nodos de almacenamiento nuevos inmediatamente.

Cuando los metadatos del objeto utilizan el 90% o más del espacio de metadatos permitido, aparece una advertencia en el panel de control. 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 **ALERTS** > **Current**.
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 agregar capacidad de metadatos a un sitio, también debe hacerlo "expanda cualquier otro sitio" Con la misma cantidad 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**.

Servicios: Estado - Alarma 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.

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un "navegador web compatible".
- Ya tienes "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.

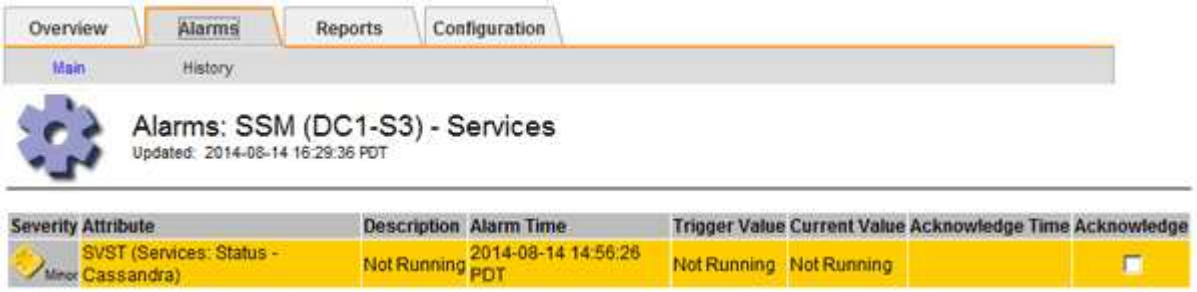
Puede hacerlo "ejecutar diagnóstico" para obtener información adicional sobre el estado actual de la cuadrícula.

> 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 siga con los pasos que se indican a continuación.

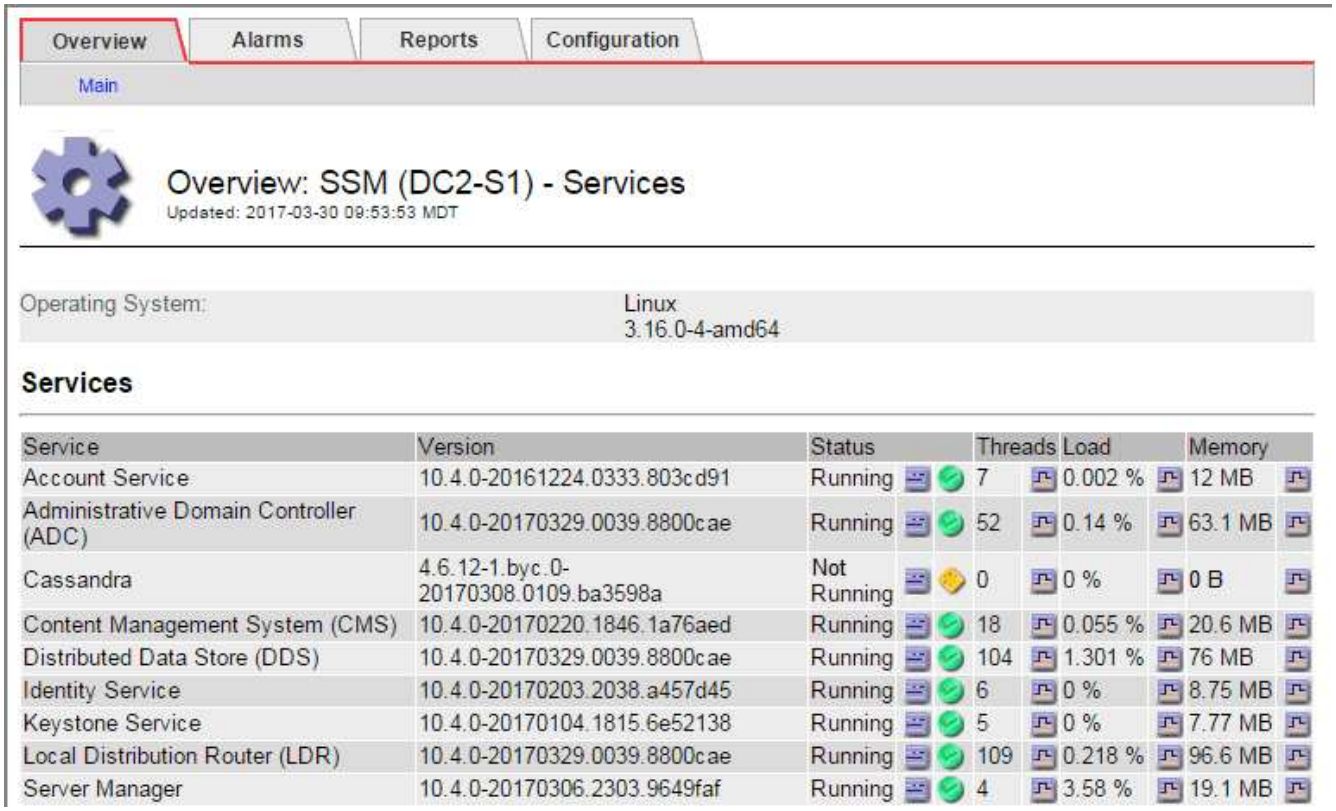
Pasos

1. Seleccione **SUPPORT** > **Tools** > **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.



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



3. 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`
4. 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.

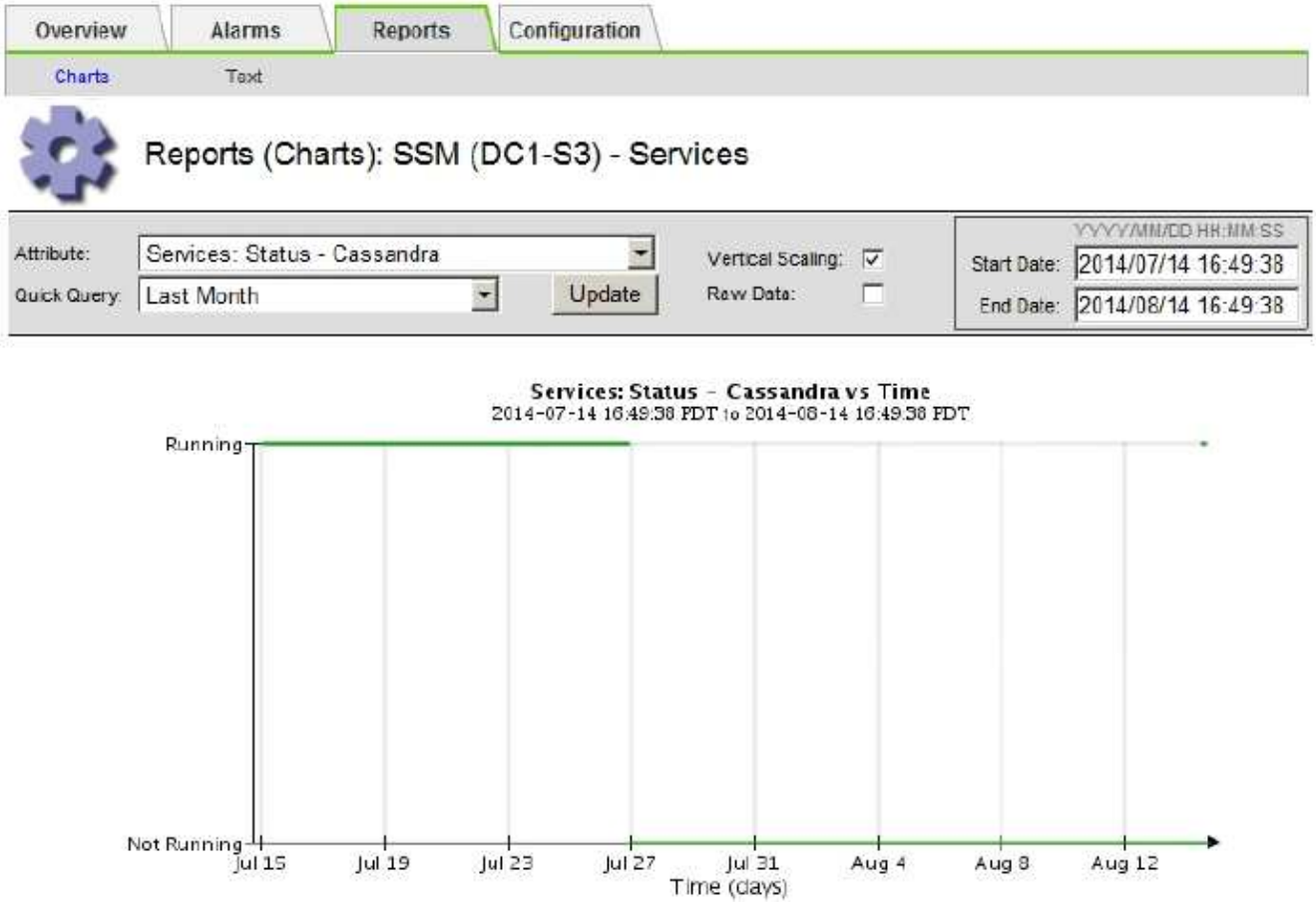
5. Para crear un gráfico en Cassandra:
   a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**. A continuación, seleccione ***Site*** > ***Storage Node*** > **SSM** > **Servicios** > **Informes** > **Cartas**.
   b. Seleccione **atributo** > **Servicio: Estado - Cassandra**.
   c. Para **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.



6. 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 ver instrucciones, consulte "Recupere el nodo de almacenamiento en más de 15 días".

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

Errores de memoria agotada de Cassandra (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. Ver el evento:
   a. Seleccione **SUPPORT** > **Tools** > **Topología de cuadrícula**.
   b. Expande el sitio y luego selecciona ***grid_node***.
   c. Seleccione **SSM**, luego seleccione **Eventos** > **Configuración**.
2. Compruebe que el número de errores de memoria de salida de Cassandra sea 1 o superior.

   Puede hacerlo "ejecutar diagnóstico" para obtener información adicional sobre el estado actual de la cuadrícula.

3. Inicie sesión en el nodo seleccionado como "admin" usando SSH y cambie al usuario raíz local.
4. Vaya a. `/var/local/core/`, comprima el `Cassandra.hprof` y envíelo al soporte técnico.
5. 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.

6. Una vez resuelto el problema, seleccione la casilla de verificación **Reset** para el recuento de errores de pila sin memoria de Cassandra. A continuación, seleccione **aplicar cambios**.

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

Solucionar 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.

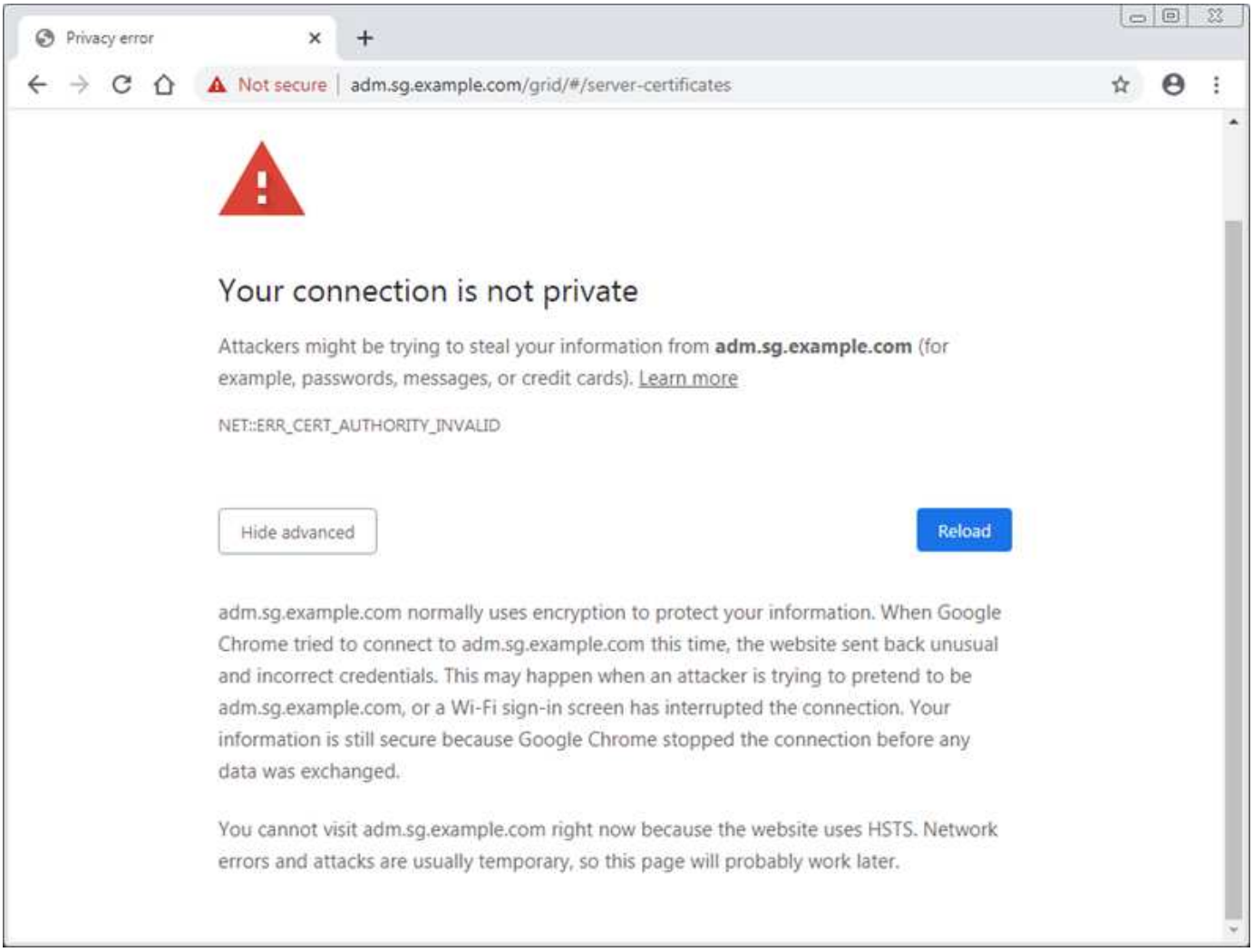
Acerca de esta tarea

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

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



Para garantizar que las operaciones no se interrumpan por un certificado de servidor fallido, la alerta **Expiración del certificado de servidor para la interfaz de administración** se activa cuando el certificado de servidor está a punto de expirar.

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

Pasos

Si ha recibido una notificación de alerta sobre un certificado caducado, acceda a los detalles del certificado: . Seleccione **CONFIGURACIÓN** > **Seguridad** > **certificados** y, a continuación "seleccione la ficha de certificado adecuada".

1. Compruebe el período de validez del certificado.
   Algunos navegadores web y clientes S3 o Swift no aceptan certificados con un período de validez superior a 398 días.
2. Si el certificado ha caducado o lo hará pronto, cargue o genere uno nuevo.
   - Para un certificado de servidor, consulte los pasos de "Configuración de un certificado de servidor personalizado para el administrador de grid y el administrador de inquilinos".
   - Para obtener un certificado de cliente, consulte los pasos de "configurar un certificado de cliente".
3. 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** > **Seguridad** > **certificados** y, a continuación, "seleccione la ficha de certificado adecuada" para instalar un nuevo certificado personalizado o continuar con el certificado predeterminado.
     iii. En las instrucciones para administrar StorageGRID, consulte los pasos para "Configuración de un certificado de servidor personalizado para el administrador de grid y el administrador de inquilinos".

Solucione 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.

Errores de inicio de sesión

Si experimenta un error al iniciar sesión en un nodo de administración de StorageGRID, es posible que el sistema tenga un problema con el "configuración de federación de identidades", a "redes" o. "hardware necesario" problema, un problema con "Servicios del nodo de administración", o un "Problema con la base de datos Cassandra" En los nodos de almacenamiento conectados.

Antes de empezar

- Usted tiene la `Passwords.txt` archivo.

- Ya tienes "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 administración 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 activado para el sistema StorageGRID, consulte los pasos para "configuración del inicio de sesión único".

   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 activado, no puede iniciar sesión con 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** > **Control de acceso** > **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 siguiente paso.
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 servicio nginx-gw se está ejecutando `# service nginx-gw status`

9. use 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.

10. Revise los siguientes registros:
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`
    - `**/*commands.txt`
11. 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.

12. 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 `#`.

13. 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.

14. Repita los pasos Utilice Lumberjack para recopilar registros y.. Revisar los registros Para revisar los registros en los nodos de almacenamiento.
15. Si no puede resolver el problema, póngase en contacto con el soporte técnico.

    Proporcione los registros recopilados al soporte técnico. Consulte también "Referencia de archivos de registro".

Problemas de la interfaz de usuario

Es posible que la interfaz de usuario de Grid Manager o del Administrador de inquilinos no responda como se espera una vez actualizado el software StorageGRID.

Pasos

1. Asegúrese de utilizar un "navegador web compatible".

   > La compatibilidad con el navegador puede cambiar con cada versión de StorageGRID. Confirme que utiliza el navegador compatible con su versión de StorageGRID.

2. 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.

Nodo de administración no disponible

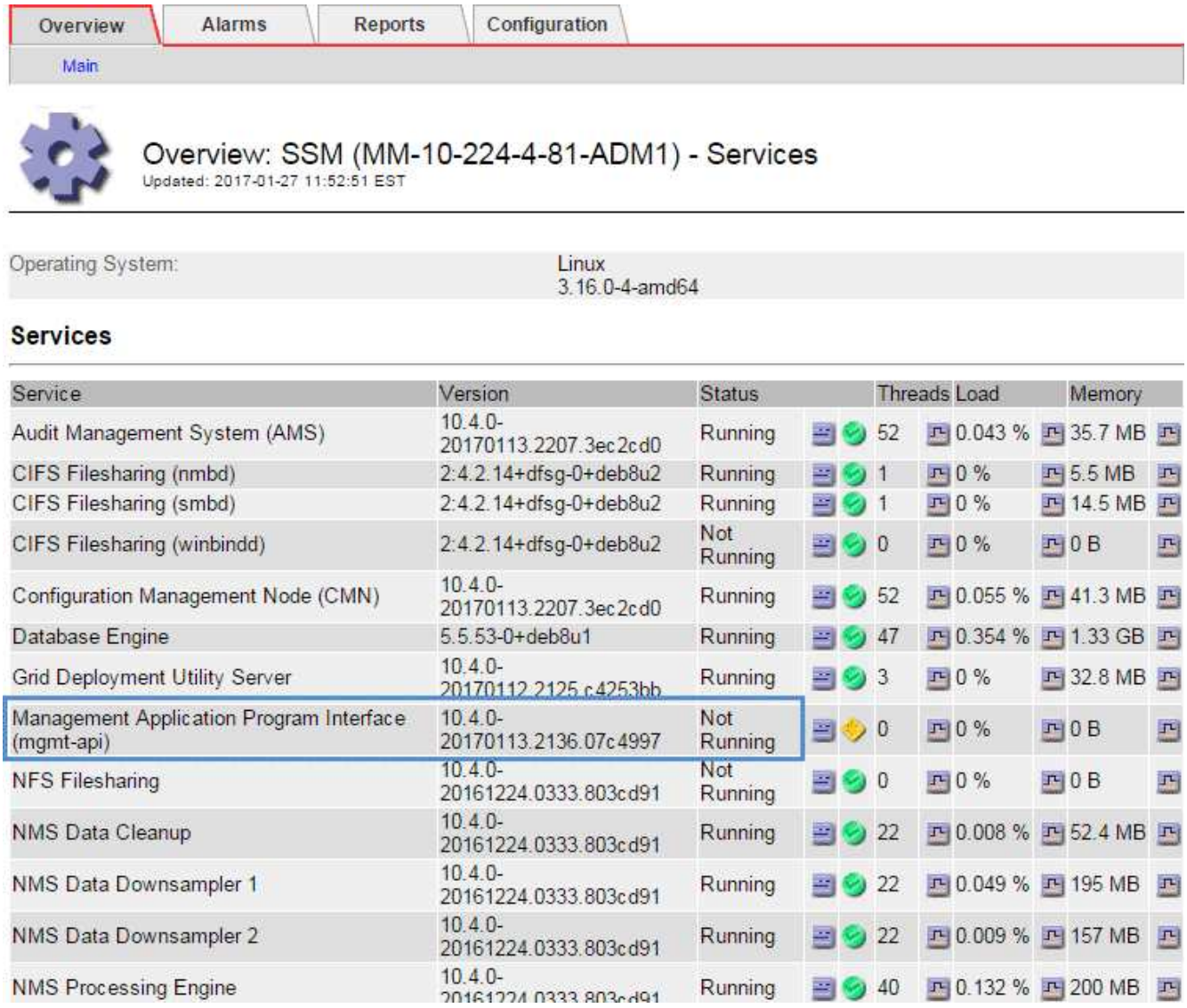
Si el sistema StorageGRID incluye varios nodos de administrador, puede usar otro nodo de administración para comprobar el estado de un nodo de administración no disponible.

Antes de empezar

Ya tienes "permisos de acceso específicos".

Pasos

1. Desde un nodo de administración disponible, inicie sesión en Grid Manager mediante un "navegador web compatible".
2. Seleccione **SUPPORT** > **Tools** > **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.



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

Solucionar 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.

Errores de «422: Entidad no procesable»

El error 422: Entidad no procesable puede ocurrir por diferentes razones. 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

`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`
	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).
	
	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.

`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)`
	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.
	
	Compruebe los códigos que ofrece el sistema externo. El sistema debe utilizar uno de los "Cifrados compatibles con StorageGRID" Para conexiones TLS salientes, como se muestra en las instrucciones para administrar StorageGRID.

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{device="eth0"}`
2. "Modifique la configuración de MTU" Según sea necesario para garantizar que son iguales para la interfaz de red de grid (eth0) en todos los nodos.
   - Para los nodos basados en Linux y VMware, use el siguiente comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

     Ejemplo: `change-ip.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-ip.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: • cuadrícula • admin • cliente

+

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

Alarma de 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.
2. Realice los siguientes pasos en función de la causa del error:

FEC no coincide

Estos pasos sólo se aplican a los errores NRER causados por la discrepancia de FEC en dispositivos StorageGRID.

a. Compruebe el estado de FEC del puerto en el interruptor conectado al dispositivo StorageGRID.
b. Compruebe la integridad física de los cables del aparato al interruptor.
c. Si desea cambiar la configuración de FEC para intentar resolver la alarma de NRER, asegúrese primero de que el aparato esté configurado para el modo **AUTO** en la página Configuración de enlace del instalador de dispositivos StorageGRID (consulte las instrucciones de su aparato:
   - "SG6160"
   - "SGF6112"
   - "SG6000"
   - "SG5800"
   - "SG5700"
   - "SG110 y SG1100"
   - "SG100 y SG1000"
d. 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 una configuración 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.

   Los dispositivos StorageGRID son compatibles con Firecode (FC) y Reed Solomon (RS) FEC, y sin FEC.

Discrepancia entre el puerto del switch y la MTU de NIC

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. No es necesario que los valores de MTU sean los mismos para todos los tipos de red. Consulte Solucione problemas de la alerta de discrepancia de MTU de red de cuadrícula si quiere más información.

Consulte también "Cambie la configuración de MTU".

Índices altos de errores de enlace

a. Active FEC, si aún no está activado.
b. Compruebe que el cableado de red es de buena calidad y que no está dañado o conectado incorrectamente.
c. 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.

Desbordamiento del búfer de anillo NIC

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.

3. Después de resolver el problema subyacente, restablezca el contador de errores.
   a. Seleccione **SUPPORT** > **Tools** > **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

"Referencia de alarmas (sistema heredado)"

Errores de sincronización de hora

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.

Cuando "Especificación del origen NTP externo" Para una instalación de StorageGRID en el nivel de producción, no use el servicio Windows Time (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.

Linux: Problemas de conectividad de red

Puede ver problemas con la conectividad de red de los nodos de 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 "Red Hat Enterprise Linux" o. "Ubuntu o Debian".

> 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 la activación de la clonación MAC, consulte las instrucciones de "Red Hat Enterprise Linux" o. "Ubuntu o Debian".

Modo promiscuo

Si no desea utilizar la clonación de direcciones MAC y prefiere permitir que todas las interfaces reciban y transmitan datos para direcciones MAC distintas de las asignadas por el hipervisor, Asegúrese de que las propiedades de seguridad en los niveles de conmutador virtual y grupo de puertos estén establecidas en **Aceptar** para el modo promiscuo, los cambios de dirección MAC y las transmisiones 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.

Para obtener más información sobre el uso del modo Promiscuous, consulte las instrucciones de "Red Hat Enterprise Linux" o. "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 del motor de contenedores para detener el contenedor de nodo 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 motor de contenedor y todos los procesos que controlan el nodo storagegrid. Por ejemplo:`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). Por ejemplo:

```
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
```

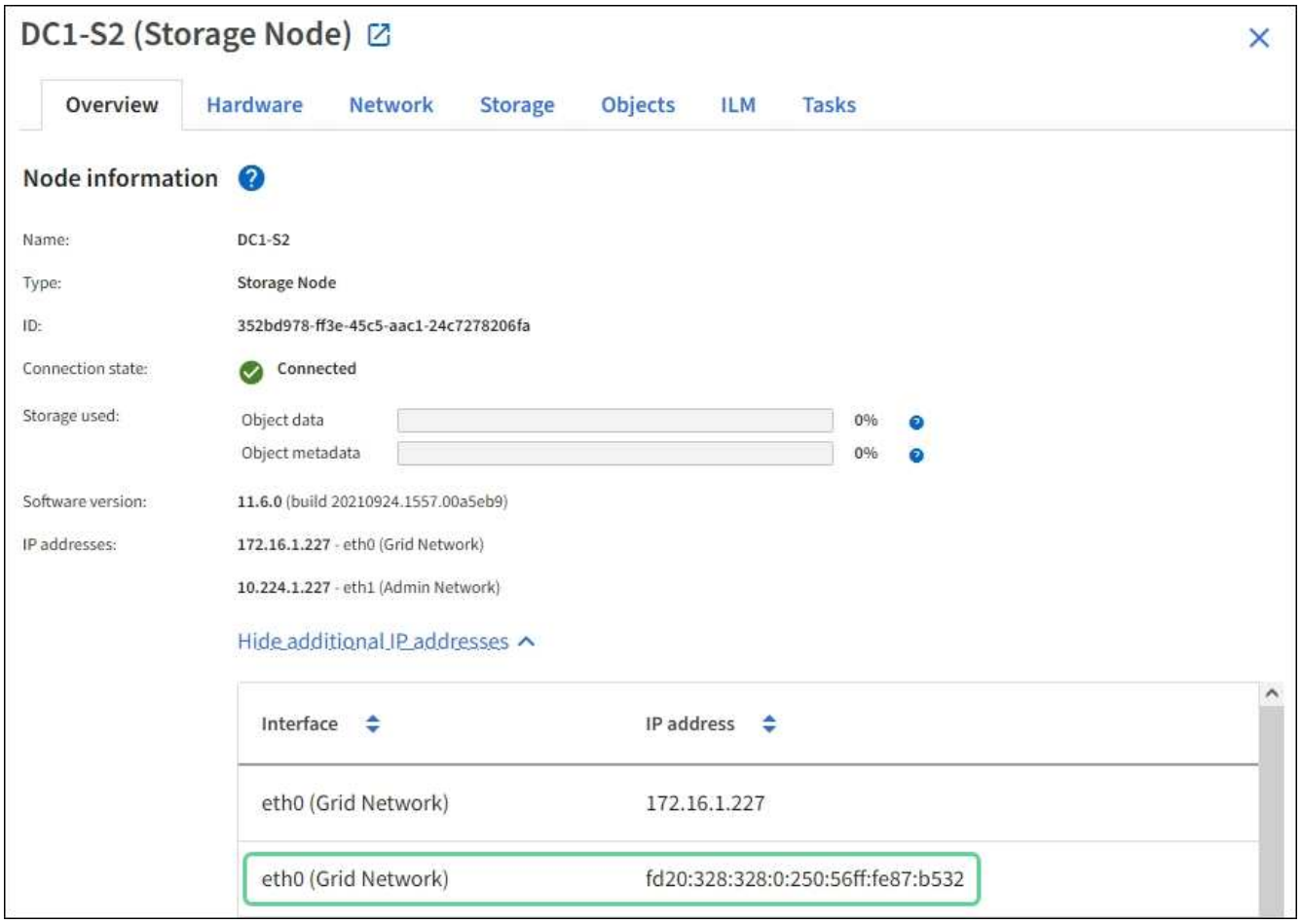
Linux: Solucione problemas de compatibilidad con IPv6

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, seleccione **Mostrar más** junto a **direcciones IP** en la ficha Descripción general.



- Seleccione **SUPPORT** > **Tools** > **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
```

Solucione problemas de un servidor de syslog externo

En la siguiente tabla, se describen los mensajes de error que pueden estar relacionados mediante un servidor de syslog externo y se enumeran las acciones correctivas.

El asistente para configurar el servidor syslog externo muestra estos errores si tiene problemas al enviar

mensajes de prueba para validar que el servidor syslog externo esté configurado correctamente.

Los problemas en tiempo de ejecución podrían ser reportados por el"Error de reenvío del servidor de syslog externo" alerta. Si recibe esta alerta, siga las instrucciones de la alerta para reenviar los mensajes de prueba para poder obtener mensajes de error detallados.

Para obtener más información sobre el envío de información de auditoría a un servidor de syslog externo, consulte:

- "Consideraciones que tener en cuenta sobre el uso de un servidor de syslog externo"
- "Configure los mensajes de auditoría y el servidor de syslog externo"

Mensaje de error	Descripción y acciones recomendadas
No se puede resolver el nombre de host	El FQDN introducido para el servidor de syslog no se pudo resolver a una dirección IP. 1. Compruebe el nombre de host que ha introducido. Si has introducido una dirección IP, asegúrate de que sea una dirección IP válida en una notación W.X.Y.Z («decimal con puntos»). 2. Compruebe que los servidores DNS están configurados correctamente. 3. Confirmar que cada nodo puede acceder a las direcciones IP del servidor DNS.
Conexión rechazada	Se rechazó una conexión TCP o TLS con el servidor de syslog. Es posible que no haya escucha de servicio en el puerto TCP o TLS del host, o que un firewall esté bloqueando el acceso. 1. Compruebe que haya introducido el FQDN o la dirección IP, el puerto y el protocolo correctos para el servidor de syslog. 2. Confirme que el host para el servicio de syslog está ejecutando un daemon de syslog que se está escuchando en el puerto especificado. 3. Confirme que un firewall no bloquea el acceso a las conexiones TCP/TLS desde los nodos a la IP y al puerto del servidor de syslog.
Red inaccesible	El servidor de syslog no está en una subred de conexión directa. Un enrutador devolvió un mensaje de error ICMP para indicar que no pudo reenviar los mensajes de prueba de los nodos enumerados al servidor de syslog. 1. Compruebe que haya introducido el FQDN o la dirección IP correctos para el servidor de syslog. 2. Para cada nodo de la lista, compruebe la lista de subredes de redes de cuadrícula, las listas de subredes de redes de administración y las puertas de enlace de red de cliente. Confirmar que se han configurado para enrutar el tráfico al servidor de syslog a través de la interfaz de red y la puerta de enlace esperadas (Grid, Admin o Client).

Mensaje de error	Descripción y acciones recomendadas
Host inaccesible	El servidor de syslog se encuentra en una subred de conexión directa (subred que utilizan los nodos mostrados para sus direcciones IP de grid, administrador o cliente). Los nodos intentaron enviar mensajes de prueba, pero no recibieron respuestas a las solicitudes ARP para la dirección MAC del servidor syslog. 1. Compruebe que haya introducido el FQDN o la dirección IP correctos para el servidor de syslog. 2. Compruebe que el host que ejecuta el servicio de syslog esté configurado.
Tiempo de espera de conexión agotado	Se ha realizado un intento de conexión TCP/TLS, pero no se ha recibido respuesta del servidor de syslog durante mucho tiempo. Es posible que haya una configuración incorrecta de enrutamiento o que un firewall esté borrando el tráfico sin enviar ninguna respuesta (una configuración común). 1. Compruebe que haya introducido el FQDN o la dirección IP correctos para el servidor de syslog. 2. Para cada nodo de la lista, compruebe la lista de subredes de redes de cuadrícula, las listas de subredes de redes de administración y las puertas de enlace de red de cliente. Confirme que están configurados para enrutar el tráfico hacia el servidor de syslog mediante la interfaz de red y la puerta de enlace (Grid, Admin o Client) mediante las que espera acceder al servidor de syslog. 3. Confirme que un firewall no bloquea el acceso a las conexiones TCP/TLS desde los nodos indicados a la IP y al puerto del servidor de syslog.
Conexión cerrada por el partner	Se estableció correctamente una conexión TCP con el servidor de syslog, pero se cerró posteriormente. Algunos motivos pueden ser: • Es posible que se haya reiniciado o reiniciado el servidor de syslog. • Es posible que el nodo y el servidor de syslog tengan diferentes ajustes de TCP/TLS. • Un firewall intermedio podría estar cerrando conexiones TCP inactivas. • Es posible que un servidor que no esté escuchando en el puerto del servidor de syslog haya cerrado la conexión. Para resolver este problema: 1. Compruebe que haya introducido el FQDN o la dirección IP, el puerto y el protocolo correctos para el servidor de syslog. 2. Si utiliza TLS, confirme que el servidor de syslog también está usando TLS. Si utiliza TCP, confirme que el servidor de syslog también utiliza TCP. 3. Compruebe que un firewall intermedio no está configurado para cerrar las conexiones TCP inactivas.

Mensaje de error	Descripción y acciones recomendadas
Error del certificado de TLS	El certificado de servidor recibido del servidor de syslog no era compatible con el paquete de certificado de CA y el certificado de cliente proporcionados. 1. Confirme que el paquete de certificado de CA y el certificado de cliente (si los hubiera) son compatibles con el certificado de servidor en el servidor de syslog. 2. Confirme que las identidades en el certificado de servidor del servidor de syslog incluyen los valores esperados de IP o FQDN.
Reenvío suspendido	Los registros de syslog ya no se reenvían al servidor de syslog y StorageGRID no puede detectar el motivo. Revise los registros de depuración proporcionados con este error para intentar determinar la causa raíz.
Sesión TLS finalizada	El servidor de syslog finalizó la sesión TLS y StorageGRID no puede detectar el motivo. 1. Revise los registros de depuración proporcionados con este error para intentar determinar la causa raíz. 2. Compruebe que haya introducido el FQDN o la dirección IP, el puerto y el protocolo correctos para el servidor de syslog. 3. Si utiliza TLS, confirme que el servidor de syslog también está usando TLS. Si utiliza TCP, confirme que el servidor de syslog también utiliza TCP. 4. Confirme que el paquete de certificado de CA y el certificado de cliente (si los hubiera) son compatibles con el certificado de servidor del servidor de syslog. 5. Confirme que las identidades en el certificado de servidor del servidor de syslog incluyen los valores esperados de IP o FQDN.
Error en la consulta de resultados	El nodo de administrador que se utiliza para la configuración y las pruebas del servidor de syslog no puede solicitar resultados de prueba a los nodos enumerados. Uno o más nodos pueden estar inactivos. 1. Siga los pasos estándar de solución de problemas para asegurarse de que los nodos estén en línea y que todos los servicios esperados estén en ejecución. 2. Reinicie el servicio miscd en los nodos indicados.

Información de copyright

Copyright © 2025 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 INTERRUPCIÓN 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.