



Solucionar problemas del sistema StorageGRID

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Solucionar problemas del sistema StorageGRID	1
Solucionar problemas de un sistema StorageGRID	1
Define el problema	1
Evaluar el riesgo y el impacto en el sistema	1
Recopilar datos	2
Analizar datos	6
Lista de verificación de información de escalada	6
Solucionar problemas de objetos y almacenamiento	8
Confirmar la ubicación de los datos de los objetos	8
Fallos en el almacén de objetos (volumen de almacenamiento)	10
Verificar la integridad del objeto	12
Solución de problemas de alerta de tamaño de objeto demasiado grande en S3 PUT	20
Solucionar problemas de datos de objetos perdidos o faltantes	22
Solucionar la alerta de almacenamiento de datos de objetos bajos	31
Solución de problemas de alertas de anulación de marca de agua de solo lectura baja	33
Solucionar problemas de metadatos	37
Solucionar errores de certificado	39
Solucionar problemas del nodo de administración y de la interfaz de usuario	40
Errores de inicio de sesión en el nodo de administración	40
Problemas de interfaz de usuario	43
Solucionar problemas de red, hardware y plataforma	44
Errores "422: Entidad no procesable"	44
Alerta de discrepancia de MTU de la red Grid	45
Alerta de error en la recepción de trama de la red del nodo	46
Errores de sincronización horaria	48
Linux: Problemas de conectividad de red	48
Linux: El estado del nodo es "huérfano"	49
Linux: Solución de problemas de compatibilidad con IPv6	50
Solucionar problemas de un servidor syslog externo	51

Solucionar problemas del sistema StorageGRID

Solucionar problemas de un sistema StorageGRID

Si encuentra un problema al usar un sistema StorageGRID , consulte los consejos y pautas de esta sección para obtener ayuda para determinar y resolver el problema.

A menudo, usted puede resolver los problemas por su cuenta; sin embargo, es posible que necesite escalar algunos asuntos al soporte técnico.

Define el problema

El primer paso para resolver un problema es definirlo claramente.

Esta tabla proporciona ejemplos de los tipos de información que puede recopilar para definir un problema:

Pregunta	Ejemplo de respuesta
¿Qué está haciendo o no haciendo el sistema StorageGRID ? ¿Cuales son sus síntomas?	Las aplicaciones cliente informan que los objetos no se pueden ingerir en StorageGRID.
¿Cuándo empezó el problema?	La ingesta de objetos se denegó por primera vez aproximadamente a las 14:50 del 8 de enero de 2020.
¿Cómo notó el problema por primera vez?	Notificado por la aplicación del cliente. También recibí notificaciones de alerta por correo electrónico.
¿El problema ocurre constantemente o sólo a veces?	El problema continúa.
Si el problema ocurre regularmente, ¿qué pasos se deben seguir para provocarlo?	El problema ocurre cada vez que un cliente intenta ingerir un objeto.
Si el problema ocurre de forma intermitente, ¿cuándo ocurre? Registre las horas de cada incidente del que tenga conocimiento.	El problema no es intermitente.
¿Has visto este problema antes? ¿Con qué frecuencia has tenido este problema en el pasado?	Esta es la primera vez que veo este problema.

Evaluar el riesgo y el impacto en el sistema

Después de haber definido el problema, evalúe su riesgo y su impacto en el sistema StorageGRID . Por ejemplo, la presencia de alertas críticas no significa necesariamente que el sistema no esté prestando servicios básicos.

Esta tabla resume el impacto que el problema de ejemplo tiene en las operaciones del sistema:

Pregunta	Ejemplo de respuesta
¿Puede el sistema StorageGRID ingerir contenido?	No.
¿Pueden las aplicaciones cliente recuperar contenido?	Algunos objetos se pueden recuperar y otros no.
¿Están en riesgo los datos?	No.
¿Se ve gravemente afectada la capacidad de realizar negocios?	Sí, porque las aplicaciones cliente no pueden almacenar objetos en el sistema StorageGRID y los datos no se pueden recuperar de manera consistente.

Recopilar datos

Después de haber definido el problema y haber evaluado su riesgo e impacto, recopile datos para su análisis. El tipo de datos que resulta más útil recopilar depende de la naturaleza del problema.

Tipo de datos a recopilar	¿Por qué recopilar estos datos?	Instrucciones
Crear una línea de tiempo de cambios recientes	Los cambios en su sistema StorageGRID , su configuración o su entorno pueden provocar un nuevo comportamiento.	• Crear una línea de tiempo de cambios recientes
Alertas de revisión	Las alertas pueden ayudarle a determinar rápidamente la causa raíz de un problema al proporcionar pistas importantes sobre los problemas subyacentes que podrían estar causándolo. Revise la lista de alertas actuales para ver si StorageGRID ha identificado la causa raíz de un problema para usted. Revise las alertas activadas en el pasado para obtener información adicional.	• "Ver alertas actuales y resueltas"
Monitorear eventos	Los eventos incluyen cualquier error del sistema o eventos de falla de un nodo, incluidos errores como errores de red. Supervise eventos para obtener más información sobre los problemas o para ayudar con la resolución de problemas.	• "Monitorear eventos"
Identificar tendencias utilizando gráficos e informes de texto	Las tendencias pueden proporcionar pistas valiosas sobre cuándo aparecieron los primeros problemas y pueden ayudarle a comprender con qué rapidez están cambiando las cosas.	• "Utilice tablas y gráficos" • "Utilice informes de texto"

Tipo de datos a recopilar	¿Por qué recopilar estos datos?	Instrucciones
Establecer líneas de base	Recopilar información sobre los niveles normales de varios valores operativos. Estos valores de referencia y las desviaciones con respecto a ellos pueden proporcionar pistas valiosas.	• Establecer líneas de base
Realizar pruebas de ingesta 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 utilizar la aplicación cliente.	• "Supervisar el rendimiento de PUT y GET"
Revisar los mensajes de auditoría	Revise los mensajes de auditoría para seguir las operaciones de StorageGRID en detalle. Los detalles en los mensajes de auditoría pueden ser útiles para solucionar muchos tipos de problemas, incluidos problemas de rendimiento.	• "Revisar los mensajes de auditoría"
Verificar la ubicación de los objetos y la integridad del almacenamiento	Si tiene problemas de almacenamiento, verifique que los objetos se coloquen donde espera. Verifique la integridad de los datos de los objetos en un nodo de almacenamiento.	• "Supervisar las operaciones de verificación de objetos" • "Confirmar la ubicación de los datos de los objetos" • "Verificar la integridad del objeto"
Recopilar datos para soporte técnico	Es posible que el soporte técnico le solicite que recopile datos o revise información específica para ayudar a solucionar problemas.	• "Recopilar archivos de registro y datos del sistema" • "Activar manualmente un paquete de AutoSupport" • "Revisar las métricas de soporte"

Crea una línea de tiempo de cambios recientes

Cuando ocurre un problema, debes considerar qué ha cambiado recientemente y cuándo ocurrieron esos cambios.

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

Cree una tabla de cambios recientes en su sistema que incluya información sobre cuándo ocurrió cada

cambio y cualquier detalle relevante sobre el cambio, como información sobre qué más estaba sucediendo mientras el cambio estaba en progreso:

Tiempo de cambio	Tipo de cambio	Detalles
Por ejemplo: • ¿Cuando comenzaste la recuperación del nodo? • ¿Cuándo se completó la actualización del software? • ¿Interrumpiste el proceso?	¿Qué pasó? ¿Qué hiciste?	Documente cualquier detalle relevante sobre el cambio. Por ejemplo: • Detalles de los cambios en la red. • ¿Qué revisión se instaló? • Cómo cambiaron las cargas de trabajo de los clientes. Asegúrese de anotar si se produjo más de un cambio al mismo tiempo. Por ejemplo, ¿se realizó este cambio mientras se estaba realizando una actualización?

Ejemplos de cambios recientes significativos

A continuación se presentan algunos ejemplos de cambios potencialmente significativos:

- ¿El sistema StorageGRID se instaló, amplió o recuperó recientemente?
- ¿Se ha actualizado el sistema recientemente? ¿Se aplicó una revisión?
- ¿Se ha reparado o cambiado algún hardware recientemente?
- ¿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 balanceadores de carga o ha agregado o eliminado un grupo de alta disponibilidad de nodos de administración o nodos de puerta de enlace?
- ¿Se ha iniciado alguna tarea que podría llevar mucho tiempo completar? Los ejemplos incluyen:
 - Recuperación de un nodo de almacenamiento fallido
 - Desmantelamiento del nodo de almacenamiento
- ¿Se han realizado cambios en la autenticación de usuarios, como agregar un inquilino o cambiar la configuración de LDAP?
- ¿Se está produciendo una migración de datos?
- ¿Se habilitaron o cambiaron recientemente los servicios de la plataforma?
- ¿Se habilitó el cumplimiento recientemente?
- ¿Se han agregado o eliminado grupos de almacenamiento en la nube?
- ¿Se han realizado cambios en la compresión o el cifrado del almacenamiento?
- ¿Ha habido algún cambio en la infraestructura de la red? Por ejemplo, VLAN, enrutadores o DNS.
- ¿Se han realizado cambios en las fuentes NTP?
- ¿Se han realizado cambios en las interfaces de red, administración o cliente?
- ¿Se han realizado otros cambios en el sistema StorageGRID o su entorno?

Establecer líneas de base

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

Propiedad	Valor	Cómo obtener
Consumo medio de almacenamiento	GB consumidos/día Porcentaje consumido/día	Vaya al Administrador de cuadrícula. En la página Nodos, seleccione toda la cuadrícula o un sitio y vaya a la pestaña Almacenamiento. En el gráfico Almacenamiento utilizado - Datos de objetos, busque un período 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 promedio de metadatos	GB consumidos/día Porcentaje consumido/día	Vaya al Administrador de cuadrícula. En la página Nodos, seleccione toda la cuadrícula o un sitio y vaya a la pestaña Almacenamiento. En el gráfico Almacenamiento utilizado - Metadatos del objeto, busque un período en el que la línea sea bastante estable. Coloque el cursor sobre el gráfico para estimar cuánto almacenamiento de metadatos se consume cada día Puede recopilar esta información para todo el sistema o para un centro de datos específico.
Tasa de operaciones S3/Swift	Operaciones/segundo	En el panel de control de Grid Manager, seleccione Rendimiento > Operaciones S3 o Rendimiento > Operaciones Swift. Para ver las tasas de ingesta y recuperación y los recuentos de un sitio o nodo específico, seleccione NODOS > sitio o Nodo de almacenamiento > Objetos. Coloque el cursor sobre el gráfico de ingesta y recuperación de S3.
Operaciones S3/Swift fallidas	Operaciones	Seleccione SOPORTE > Herramientas > Topología de cuadrícula. En la pestaña Descripción general de la sección Operaciones de API, vea el valor de Operaciones S3 - Fallidas u Operaciones Swift - Fallidas.

Propiedad	Valor	Cómo obtener
Tasa de evaluación de ILM	Objetos/segundo	Desde la página Nodos, seleccione grid > ILM . En el gráfico de cola ILM, busque un período en el que la línea sea bastante estable. Coloque el cursor sobre el gráfico para estimar un valor de referencia para la Tasa de evaluación para su sistema.
Velocidad de escaneo ILM	Objetos/segundo	Seleccione NODOS > grid > ILM . En el gráfico de cola ILM, busque un período en el que la línea sea bastante estable. Coloque el cursor sobre el gráfico para estimar un valor de referencia para la velocidad de escaneo para su sistema.
Objetos en cola de las operaciones del cliente	Objetos/segundo	Seleccione NODOS > grid > ILM . En el gráfico de cola ILM, busque un período en el que la línea sea bastante estable. Coloque el cursor sobre el gráfico para estimar un valor de referencia para Objetos en cola (de operaciones del cliente) para su sistema.
Latencia promedio de consulta	Milisegundos	Seleccione NODOS > Nodo de almacenamiento > Objetos . En la tabla Consultas, vea el valor de Latencia promedio.

Analizar datos

Utilice la información que recopile para determinar la causa del problema y las posibles soluciones.

El análisis depende del problema, pero en general:

- Localice puntos de fallo y cuellos de botella utilizando las alertas.
- Reconstruya el historial de problemas utilizando el historial de alertas y los gráficos.
- Utilice gráficos para encontrar anomalías y comparar la situación del problema con el funcionamiento normal.

Lista de verificación de información de escalada

Si no puede resolver el problema por su cuenta, comuníquese con el soporte técnico. Antes de contactar con el soporte técnico, reúna la información que aparece en la siguiente tabla para facilitar la resolución del problema.

	Artículo	Notas
	Planteamiento del problema	¿Cuales son los síntomas del problema? ¿Cuando empezó el problema? ¿Sucede de manera constante o intermitente? Si es intermitente, ¿cuándo ha ocurrido? Definir el problema
	Evaluación de impacto	¿Cuál es la gravedad del problema? ¿Cuál es el impacto en la aplicación cliente? • ¿El cliente se ha conectado exitosamente anteriormente? • ¿Puede el cliente ingerir, recuperar y eliminar datos?
	ID del sistema StorageGRID	Seleccione MANTENIMIENTO > Sistema > Licencia. El ID del sistema StorageGRID se muestra como parte de la licencia actual.
	Versión del software	Desde la parte superior del Administrador de cuadrícula, seleccione el ícono de ayuda y seleccione Acerca de para ver la versión de StorageGRID .
	Personalización	Resuma cómo está configurado su sistema StorageGRID . Por ejemplo, enumera lo siguiente: • ¿La red utiliza compresión de almacenamiento, cifrado de almacenamiento o cumplimiento? • ¿ILM fabrica objetos replicados o codificados por borrado? ¿ILM garantiza la redundancia del sitio? ¿Las reglas de ILM utilizan los comportamientos de ingesta de confirmación equilibrada, estricta o dual?
	Archivos de registro y datos del sistema	Recopile archivos de registro y datos del sistema para su sistema. Seleccione SOPORTE > Herramientas > Registros. Puede recopilar registros para toda la red o para nodos seleccionados. Si está recopilando registros solo para nodos seleccionados, asegúrese de incluir al menos un nodo de almacenamiento que tenga el servicio ADC. (Los primeros tres nodos de almacenamiento de un sitio incluyen el servicio ADC). "Recopilar archivos de registro y datos del sistema"

	Artículo	Notas
	Información de referencia	Recopilar información de referencia sobre las operaciones de ingesta, las operaciones de recuperación y el consumo de almacenamiento. Establecer líneas de base
	Cronología de cambios recientes	Cree una línea de tiempo que resuma todos los cambios recientes en el sistema o 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 usted mismo, asegúrese de registrar los pasos que siguió y el resultado.

Solucionar problemas de objetos y almacenamiento

Confirmar la ubicación de los datos de los objetos

Dependiendo del problema, es posible que desees ["confirmar dónde se almacenan los datos del objeto"](#) . Por ejemplo, es posible que desee verificar que la política ILM esté funcionando como se espera y que los datos de los objetos se estén almacenando donde corresponde.

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 mayúsculas.
 - **CBID**: El identificador único del objeto dentro de StorageGRID . Puede obtener el CBID de un objeto desde el registro de auditoría. Introduzca el CBD en mayúsculas.
 - **Clave de objeto y depósito S3**: cuando se ingiere un objeto a través de ["Interfaz S3"](#) La aplicación cliente utiliza una combinación de clave de objeto y depósito 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**.

Puede ingresar un UUID, CBID, clave de objeto/depósito S3 o nombre de objeto/contenedor Swift.

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

Object Metadata Lookup

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

Identifier:

Version ID (optional):

4. Seleccione **Buscar**.

El "resultados de la búsqueda de metadatos de objetos" aparecer. En esta página se enumeran los siguientes tipos de información:

- Metadatos del sistema, incluido el ID del objeto (UUID), el ID de la versión (opcional), el nombre del objeto, el nombre del contenedor, el nombre o ID de la cuenta del inquilino, el tamaño lógico del objeto, la fecha y hora en que se creó el objeto por primera vez y la fecha y hora en que se modificó el objeto por última vez.
- Cualquier par clave-valor de metadatos de usuario personalizados asociados con el objeto.
- Para los objetos S3, cualquier par clave-valor de etiqueta de objeto asociado con el objeto.
- Para copias de objetos replicados, la ubicación de almacenamiento actual de cada copia.
- Para las copias de objetos con código de borrado, la ubicación de almacenamiento actual de cada fragmento.
- Para las copias de objetos en un grupo de almacenamiento en la nube, la ubicación del objeto, incluido el nombre del depósito externo y el identificador único del objeto.
- Para objetos segmentados y objetos multiparte, una lista de segmentos de objetos que incluye identificadores de segmento y tamaños de datos. Para los objetos con más de 100 segmentos, solo se muestran los primeros 100 segmentos.
- Todos los metadatos del objeto en el formato de almacenamiento interno sin procesar. Estos metadatos sin procesar incluyen metadatos internos del sistema que no se garantiza que persistan de una versión a otra.

El siguiente ejemplo muestra los resultados de la búsqueda de metadatos de un objeto de prueba S3 que se almacena 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": {
      "PAHS": "2",

```

Fallos en el 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.

Puede ver información del almacén de objetos para 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

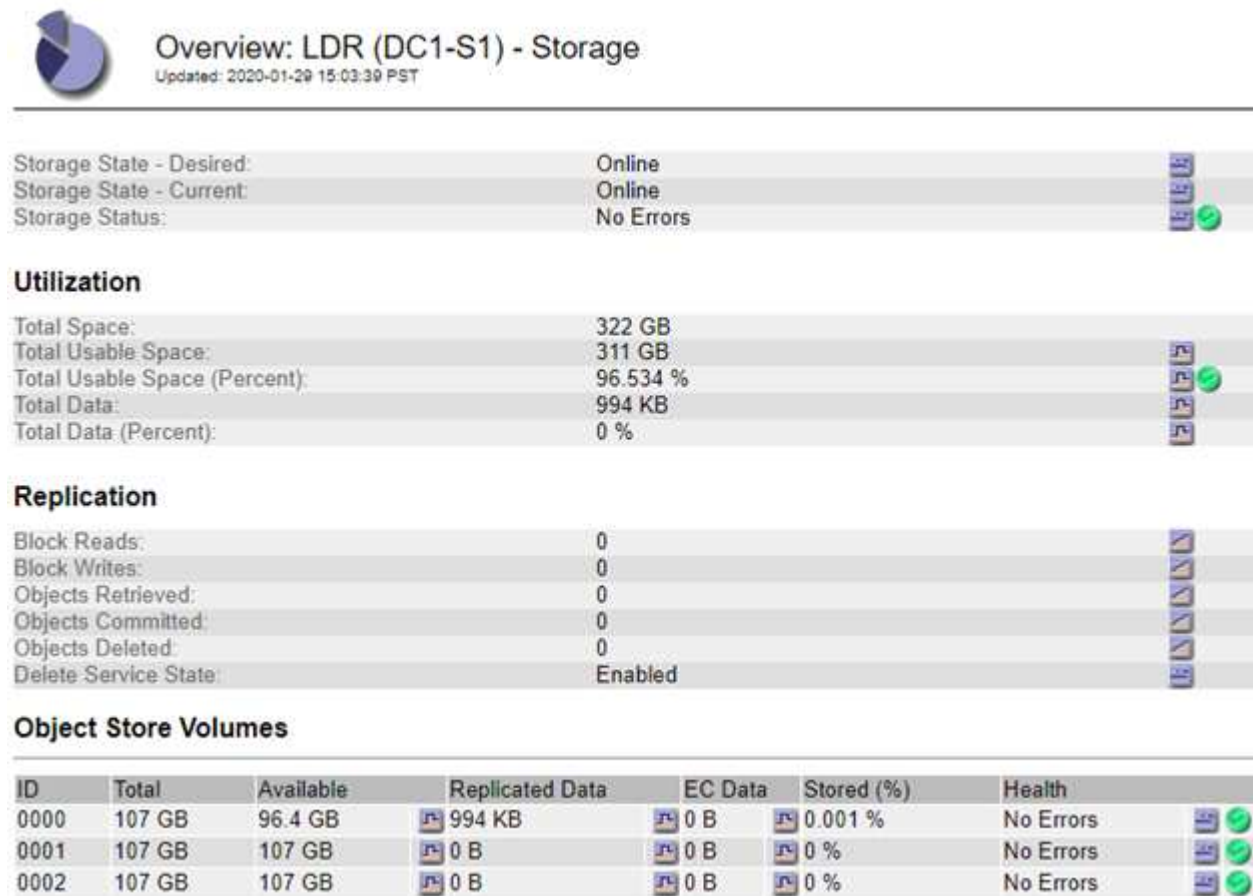
Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2	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 sobre cada nodo de almacenamiento"](#) , siga estos pasos:

1. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
2. Seleccione **sitio > Nodo de almacenamiento > LDR > Almacenamiento > Descripción general > Principal**.



Dependiendo de la naturaleza de la falla, las fallas en un volumen de almacenamiento podrían reflejarse en ["alertas de volumen de almacenamiento"](#) . Si falla un volumen de almacenamiento, debe repararlo para restaurar el nodo de almacenamiento a su funcionalidad completa lo antes posible. Si es necesario, puede ir a la pestaña **Configuración** y ["Coloque el nodo de almacenamiento en un estado de solo lectura"](#) para que el sistema StorageGRID pueda usarlo para la recuperación de datos mientras se prepara para una recuperación completa del servidor.

Verificar la integridad del objeto

El sistema StorageGRID verifica la integridad de los datos de los objetos en los nodos de almacenamiento, comprobando si hay objetos dañados o faltantes.

Hay dos procesos de verificación: verificación en segundo plano y verificación de existencia de objetos (antes llamada verificación en primer plano). Trabajan juntos para garantizar la integridad de los datos. La verificación de antecedentes se ejecuta automáticamente y verifica continuamente la exactitud de los datos del objeto. Un usuario puede activar la verificación de existencia de objetos para verificar más rápidamente la existencia (aunque no la exactitud) de los objetos.

¿Qué es la verificación de antecedentes?

El proceso de verificación en segundo plano verifica de manera automática y continua los nodos de almacenamiento en busca de copias corruptas de datos de objetos e intenta reparar automáticamente cualquier problema que encuentre.

La verificación de antecedentes verifica la integridad de los objetos replicados y los objetos codificados por 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 elimina de su ubicación y se pone en cuarentena en otro lugar del nodo de almacenamiento. Luego, se genera una nueva copia no dañada y se coloca para satisfacer las políticas 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 pueda acceder a ellos. Para obtener más información sobre cómo acceder a los datos de objetos en cuarentena, comuníquese con el soporte técnico.

- **Objetos con código de borrado:** si el proceso de verificación en segundo plano detecta que un fragmento de un objeto con código de borrado está dañado, StorageGRID intenta automáticamente reconstruir el fragmento faltante en su lugar en el mismo nodo de almacenamiento, utilizando los datos restantes y los fragmentos de paridad. Si no se puede reconstruir el fragmento dañado, se intenta recuperar otra copia del objeto. Si la recuperación es exitosa, se realiza una evaluación ILM para crear una copia de reemplazo del objeto codificado por borrado.

El proceso de verificación de fondo verifica objetos únicamente en los nodos de almacenamiento. No verifica objetos en un grupo de almacenamiento en la nube. Los objetos deben tener más de cuatro días para calificar para la verificación de antecedentes.

La verificación de antecedentes se ejecuta a un ritmo continuo que está diseñado para no interferir con las actividades normales del sistema. La verificación de antecedentes no se puede detener. Sin embargo, puede aumentar la tasa de verificación de fondo para verificar más rápidamente el contenido de un nodo de almacenamiento si sospecha que hay un problema.

Alertas relacionadas con la verificación de antecedentes

Si el sistema detecta un objeto corrupto que no puede corregir automáticamente (porque la corrupción impide identificar el objeto), se activa la alerta **Objeto corrupto no identificado detectado**.

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

Cambiar la tasa de verificación de antecedentes

Puede cambiar la velocidad a la que la verificación de fondo verifica los datos de objetos replicados en un nodo de almacenamiento si tiene inquietudes sobre la integridad de los datos.

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).

Acerca de esta tarea

Puede cambiar la tasa de verificación para la verificación de antecedentes en un nodo de almacenamiento:

- **Adaptable:** configuración predeterminada. La tarea está diseñada para verificar a un máximo de 4 MB/s o 10 objetos/s (lo que se exceda primero).
- **Alto:** la verificación del almacenamiento se realiza rápidamente, a un ritmo que puede ralentizar las actividades normales del sistema.

Utilice la tasa de verificación alta solo cuando sospeche que una falla de hardware o software podría haber dañado los datos del objeto. Una vez completada la verificación de antecedentes de alta prioridad, la tasa de verificación se restablece automáticamente a Adaptable.

Pasos

1. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
2. Seleccione **Nodo de almacenamiento > LDR > Verificación**.
3. Seleccione **Configuración > Principal**.
4. Vaya a **LDR > Verificación > Configuración > Principal**.
5. En Verificación de antecedentes, seleccione **Tasa de verificación > Alta** o **Tasa de verificación > Adaptativa**.

Overview Alarms Reports Configuration

Main

Configuration: LDR (Storage Grid) - Verification
Updated: 2021-11-11 07:13:00 MST

Reset Missing Objects Count ☐

Background Verification

Verification Rate Adaptive

Reset Corrupt Objects Count ☐

Quarantined Objects

Delete Quarantined Objects ☐

Apply Changes

6. Haga clic en **Aplicar cambios**.
7. Supervisar los resultados de la verificación en segundo plano de los objetos replicados.
 - a. Vaya a **NODOS > Nodo de almacenamiento > Objetos**.
 - 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 objetos replicados corruptos, se incrementa la métrica **Objetos corruptos** y StorageGRID intenta extraer el identificador del 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 lugar del sistema StorageGRID que satisfaga las políticas ILM activas.
- Si no se puede extraer el identificador del objeto (porque está dañado), se incrementa la métrica **Objetos dañados no identificados** y se activa la alerta **Objeto dañado no identificado detectado**.

c. Si se encuentran datos de objetos replicados dañados, comuníquese con el soporte técnico para determinar la causa raíz de la corrupción.

8. Supervisar los resultados de la verificación de antecedentes para objetos con código de borrado.

Si la verificación de fondo encuentra fragmentos corruptos de datos de objetos codificados para borrado, se incrementa el atributo Fragmentos corruptos detectados. StorageGRID se recupera reconstruyendo el fragmento dañado en el mismo nodo de almacenamiento.

a. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.

b. Seleccione **Nodo de almacenamiento > LDR > Codificación de borrado**.

c. En la tabla Resultados de verificación, supervise el atributo Fragmentos corruptos detectados (ECCD).

9. Una vez que el sistema StorageGRID haya restaurado automáticamente los objetos corruptos, restablezca el recuento de objetos corruptos.

a. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.

b. Seleccione **Nodo de almacenamiento > LDR > Verificación > Configuración**.

c. Seleccione **Restablecer recuento de objetos corruptos**.

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**, es posible que el soporte técnico desee acceder a los objetos en cuarentena para ayudar a depurar el problema subyacente o intentar recuperar datos.

a. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.

b. Seleccione **Nodo de almacenamiento > LDR > Verificación > Configuración**.

c. Seleccione **Eliminar objetos en cuarentena**.

d. Seleccione **Aplicar cambios**.

¿Qué es la comprobación de existencia de objetos?

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

A diferencia de la verificación de antecedentes, que se realiza automáticamente, debe iniciar manualmente un trabajo de verificación de existencia de objetos.

La verificación de existencia de objetos lee los metadatos de cada objeto almacenado en StorageGRID y verifica la existencia de copias de objetos replicados y fragmentos de objetos codificados para borrado. Cualquier dato faltante se gestiona de la siguiente manera:

- **Copias replicadas:** si falta una copia de los datos del objeto replicado, StorageGRID intenta automáticamente reemplazar la copia desde una copia almacenada en otra parte del sistema. El nodo de almacenamiento ejecuta una copia existente a través de una evaluación ILM, que determinará que la política ILM actual ya no se cumple para este objeto porque falta otra copia. Se genera una nueva copia y se coloca para satisfacer las políticas ILM activas del sistema. Es posible que esta nueva copia no esté colocada en el mismo lugar donde se almacenó la copia faltante.
- **Fragmentos codificados por borrado:** si falta un fragmento de un objeto codificado por borrado, StorageGRID intenta automáticamente reconstruir el fragmento faltante en su lugar en el mismo nodo de almacenamiento usando los fragmentos restantes. Si el fragmento faltante 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 con código de borrado.

Ejecutar comprobación de existencia de objeto

Crea y ejecuta un trabajo de verificación de existencia de objeto a la vez. Cuando crea un trabajo, selecciona los nodos de almacenamiento y los volúmenes que desea verificar. También selecciona la consistencia del trabajo.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de mantenimiento o acceso root"](#) .
- Se ha asegurado de que los nodos de almacenamiento que desea comprobar estén en línea. Seleccione **NODOS** para ver la tabla de nodos. Asegúrese de que no aparezcan íconos de alerta junto al nombre del nodo que desea verificar.
- Se ha asegurado de que los siguientes procedimientos **no** se estén ejecutando en los nodos que desea comprobar:
 - Expansión de la red para agregar un nodo de almacenamiento
 - Desmantelamiento del nodo de almacenamiento
 - Recuperación de un volumen de almacenamiento fallido
 - Recuperación de un nodo de almacenamiento con una unidad de sistema defectuosa
 - Reequilibrio de la CE
 - Clon de nodo de dispositivo

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

Acerca de esta tarea

Una tarea de verificación de existencia de un objeto puede tardar días o semanas en completarse, dependiendo de la cantidad de objetos en la cuadrícula, los nodos y volúmenes de almacenamiento seleccionados y la consistencia seleccionada. Puede ejecutar solo un trabajo a la vez, pero puede seleccionar varios nodos de almacenamiento y volúmenes al mismo tiempo.

Pasos

1. Seleccione **MANTENIMIENTO > Tareas > Comprobación de existencia de objetos**.
2. Seleccione **Crear trabajo**. Aparece el asistente para crear un trabajo de verificación de existencia de objetos.
3. Seleccione los nodos que contienen los volúmenes que desea verificar. Para seleccionar todos los nodos en línea, seleccione la casilla de verificación **Nombre del nodo** en el encabezado de la columna.

Puede buscar por nombre de nodo o sitio.

No puedes seleccionar nodos que no estén conectados a la red.

4. Seleccione **Continuar**.

5. Seleccione uno o más volúmenes para cada nodo de la lista. Puede buscar volúmenes utilizando el número de volumen de almacenamiento o el nombre del nodo.

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

6. Seleccione **Continuar**.

7. Seleccione la consistencia para el trabajo.

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

- **Sitio fuerte:** Dos copias de metadatos en un solo sitio.
- **Fuerte-global:** Dos copias de metadatos en cada sitio.
- **Todos** (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 en el asistente para actualizar sus selecciones.

Se genera un trabajo de verificación de existencia de objeto y se ejecuta hasta que ocurre una de las siguientes situaciones:

- El trabajo está terminado.
- Pausa o cancela el trabajo. Puedes reanudar un trabajo que hayas pausado, pero no puedes reanudar un trabajo que hayas cancelado.
- El trabajo se estanca. Se activa la alerta **La comprobación de existencia del objeto se ha estancado**. Siga las acciones correctivas especificadas para la alerta.
- El trabajo falla. Se activa la alerta **La comprobación de existencia del objeto ha fallado**. Siga las acciones correctivas especificadas para la alerta.
- Aparece un mensaje de "Servicio no disponible" o "Error interno del servidor". Después de un minuto, actualice la página para continuar monitoreando el trabajo.



Según sea necesario, puede salir de la página de verificación de existencia de objetos y regresar para continuar monitoreando el trabajo.

10. A medida que se ejecuta el trabajo, observe la pestaña **Trabajo activo** y anote el valor de Copias de objetos faltantes detectadas.

Este valor representa el número total de copias faltantes de objetos replicados y objetos con código de borrado con uno o más fragmentos faltantes.

Si la cantidad de copias de objetos faltantes detectadas es mayor a 100, es posible que haya un problema con el almacenamiento del nodo de almacenamiento.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job

Job history

Status: Accepted

Consistency control: All

Job ID: 2334602652907829302

Start time: 2021-11-10 14:43:02 MST

Missing object copies detected: 0

Elapsed time: —

Progress: 0%

Estimated time to completion: —

Pause

Cancel

Volumes

Details

Selected node	Selected storage volumes	Site
DC1-S1	0, 1, 2	Data Center 1
DC1-S2	0, 1, 2	Data Center 1
DC1-S3	0, 1, 2	Data Center 1

11. Una vez finalizado el trabajo, tome las medidas adicionales necesarias:

- Si las copias de objetos faltantes detectadas son cero, entonces no se encontraron problemas. No se requiere ninguna acción
- Si la cantidad de copias de objetos faltantes detectadas es mayor que cero y no se ha activado la alerta **Objetos perdidos**, el sistema habrá reparado todas las copias faltantes. Verifique que se hayan corregido todos los problemas de hardware para evitar daños futuros a las copias de objetos.
- Si la cantidad de copias de objetos faltantes detectadas es mayor que 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 copias de objetos perdidos utilizando grep para extraer los mensajes de auditoría de LLST: `grep LLST audit_file_name`.

Este procedimiento es similar al de "investigando objetos perdidos", aunque para las copias de objetos se busca LLST en lugar de OLSST.

12. Si seleccionó la consistencia de sitio fuerte o global fuerte para el trabajo, espere aproximadamente tres semanas para que haya consistencia de metadatos y luego vuelva a ejecutar el trabajo en los mismos volúmenes.

Cuando StorageGRID haya tenido tiempo de lograr la consistencia de metadatos para los nodos y volúmenes incluidos en el trabajo, volver a ejecutar el trabajo podría borrar copias de objetos faltantes informadas erróneamente o hacer que se verifiquen copias de objetos adicionales si se omitieron.

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

- b. Determinar qué trabajos están listos para volver a ejecutarse:
 - i. Mire la columna **Hora de finalización** para determinar qué trabajos se ejecutaron hace más de tres semanas.
 - ii. Para esos trabajos, escanee la columna de control de consistencia en busca de sitios fuertes o globales fuertes.
- c. Seleccione la casilla de verificación para cada trabajo que desee volver a ejecutar y luego seleccione **Reejecutar**.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job | Job history

Delete | **Rerun** | Search by Job ID/ node name/ consistency control/ start time

Displaying 4 results

☐	Job ID	Status	Nodes (volumes)	Missing object copies detected	Consistency control	Start time	End time
☒	2334602652907829302	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and 7 more	0	All	2021-11-10 14:43:02 MST	2021-11-10 14:43:06 MST (3 weeks ago)
☐	11725651898848823235 (Rerun job)	Completed	DC1-S2 (2 volumes) DC1-S3 (2 volumes) DC1-S4 (2 volumes) and 4 more	0	Strong-site	2021-11-10 14:42:10 MST	2021-11-10 14:42:11 MST (17 minutes ago)

- d. En el asistente para volver a ejecutar trabajos, revise los nodos y volúmenes seleccionados y la consistencia.
- e. Cuando esté listo para volver a ejecutar los trabajos, seleccione **Reejecutar**.

Aparece la pestaña Trabajo activo. Todos los trabajos que seleccionó se vuelven a ejecutar como un solo trabajo con una consistencia de sitio sólido. Un campo **Trabajos relacionados** en la sección Detalles enumera los ID de los trabajos originales.

Después de terminar

Si aún tiene inquietudes sobre la integridad de los datos, vaya a **SOPORTE > Herramientas > Topología de cuadrícula > sitio > Nodo de almacenamiento > LDR > Verificación > Configuración > Principal** y aumente la tasa de verificación en segundo plano. La verificación de antecedentes verifica la exactitud de todos los datos de los objetos almacenados y repara cualquier problema que encuentre. Encontrar y reparar problemas potenciales lo más rápido posible reduce el riesgo de pérdida de datos.

Solución de problemas de alerta de tamaño de objeto demasiado grande en S3 PUT

La alerta de tamaño de objeto PUT de S3 demasiado grande se activa si un inquilino intenta una operación PutObject que no sea multiparte y que exceda el límite de tamaño de S3 de 5 GiB.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .

Determina qué inquilinos usan objetos de más de 5 GiB para poder notificarles.

Pasos

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

- a. Ingresar `ssh admin@primary_Admin_Node_IP`
- b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

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

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

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

Opción	Destino
Nodos locales (predeterminado)	<code>/var/local/log/localaudit.log</code>
Nodos de administración/nodos locales	• Nodos de administración (principales y no principales): <code>/var/local/audit/export/audit.log</code> • Todos los nodos: El <code>/var/local/log/localaudit.log</code> En este modo, el archivo normalmente está vacío o falta.
Servidor syslog externo	<code>/var/local/log/localaudit.log</code>

Dependiendo de la configuración de destino de su auditoría, ingrese: `cd /var/local/log o /var/local/audit/export/`

Para obtener más información, consulte ["Seleccionar destinos de información de auditoría"](#) .

- f. Identifique qué inquilinos utilizan objetos de más de 5 GiB.
 - i. Ingresar `zgrep SPUT * | egrep "CSIZ\ (UI64\) : ([5-9] | [1-9] [0-9]+) [0-9] {9} "`

- ii. Para cada mensaje de auditoría en los resultados, consulte S3AI campo para determinar el ID de la cuenta del inquilino. Utilice los demás campos del mensaje para determinar qué dirección IP utilizaron el cliente, el depósito y el objeto:

Código	Descripción
SAIP	IP de origen
S3AI	Identificación del inquilino
S3BK	Balde
S3KY	Objeto
CSIZ	Tamaño (bytes)

Ejemplo de resultados del registro de auditoría

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"060X85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(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):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Si las escrituras del cliente no son normales, utilice el ID del inquilino de la alerta para identificar al inquilino:
- Vaya a **SOPORTE > Herramientas > Registros**. Recopilar registros de aplicaciones para el nodo de almacenamiento en la alerta. Especifique 15 minutos antes y después de la alerta.
 - Extrae el archivo y ve a `bycast.log`:

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

- Buscar en el registro `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 deben utilizar cargas multiparte para objetos mayores a 5 GiB.
5. Ignore la alerta durante una semana si se ha modificado la aplicación.

Solucionar problemas de datos de objetos perdidos o faltantes

Solucionar problemas de datos de objetos perdidos o faltantes

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

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

Si esta recuperación es exitosa, el sistema StorageGRID reemplaza la copia faltante del objeto. De lo contrario, se activa la alerta **Objetos perdidos**, de la siguiente manera:

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

Debe investigar todas las alertas de **Objetos perdidos** inmediatamente para determinar la causa raíz de la pérdida y si el objeto aún podría existir en un nodo de almacenamiento fuera de línea o que no esté disponible en ese momento. Ver ["Investigar objetos perdidos"](#).

En el caso de que se pierdan datos de objetos sin copias, no existe solución de recuperación. Sin embargo, debe restablecer el contador de objetos perdidos para evitar que los objetos perdidos conocidos enmascaren cualquier objeto perdido nuevo. Ver ["Restablecer el recuento de objetos perdidos y faltantes"](#).

Investigar objetos perdidos

Cuando se activa la alerta **Objetos perdidos**, debes investigar de inmediato. Recopile información sobre los objetos afectados y comuníquese con el soporte técnico.

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).

- Debes tener el `Passwords.txt` archivo.

Acerca de esta tarea

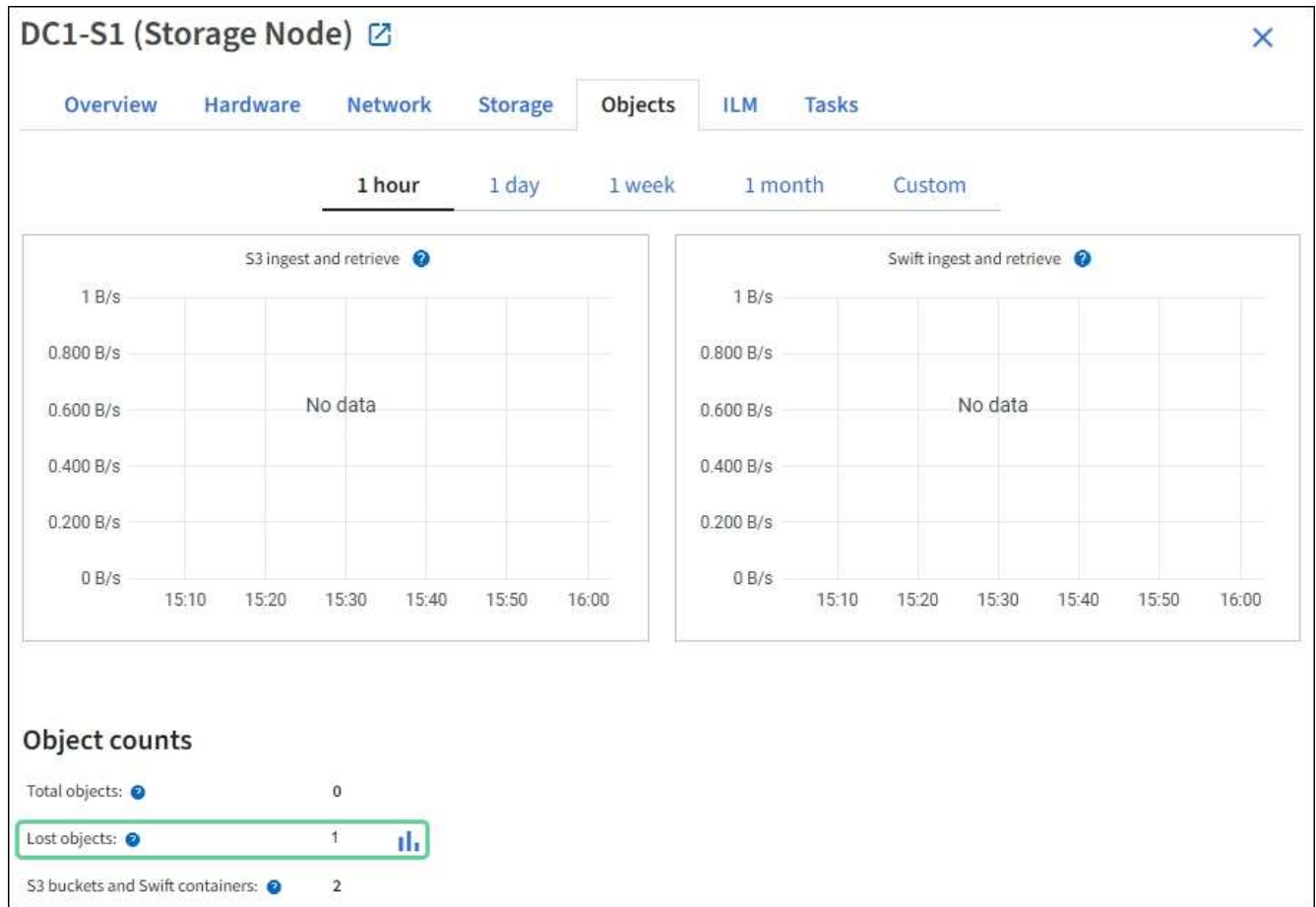
La alerta **Objetos perdidos** indica que StorageGRID cree que no hay copias de un objeto en la red. Es posible que se hayan perdido datos de forma permanente.

Investigar inmediatamente las alertas de objetos perdidos. Es posible que sea necesario tomar medidas para evitar una mayor pérdida de datos. En algunos casos, es posible que puedas recuperar un objeto perdido si actúas con rapidez.

Pasos

1. Seleccione **NODOS**.
2. Seleccione **Nodo de almacenamiento > Objetos**.
3. Revise la cantidad de objetos perdidos que se muestran en la tabla de recuento de objetos.

Este número indica la cantidad total de objetos que este nodo de la cuadrícula detecta como faltantes en 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, "[acceder 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 la red:
 - i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

- iii. Introduzca el siguiente comando para cambiar a root: `su -`
 - iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo. Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.
- b. Cambie al directorio donde se encuentran los registros de auditoría.

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

Opción	Destino
Nodos locales (predeterminado)	<code>/var/local/log/localaudit.log</code>
Nodos de administración/nodos locales	• Nodos de administración (principales y no principales): <code>/var/local/audit/export/audit.log</code> • Todos los nodos: El <code>/var/local/log/localaudit.log</code> En este modo, el archivo normalmente está vacío o falta.
Servidor syslog externo	<code>/var/local/log/localaudit.log</code>

Dependiendo de la configuración de destino de su auditoría, ingrese: `cd /var/local/log` o `/var/local/audit/export/`

Para obtener más información, consulte ["Seleccionar destinos de información de auditoría"](#).

- c. Utilice `grep` para extraer los mensajes de auditoría de Objeto Perdido (OLST). Ingrese: `grep OLST audit_file_name`
- d. Tenga en cuenta el valor 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][AMID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Busque los metadatos del objeto perdido utilizando el UUID:
 - a. Seleccione **ILM > Búsqueda de metadatos de objetos**.
 - b. Ingrese el UUID y seleccione **Buscar**.
 - c. Revise las ubicaciones en los metadatos y tome la acción adecuada:

Metadatos	Conclusión
Objeto <object_identifier> no encontrado	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 fue eliminado intencionalmente.
Ubicaciones > 0	Si hay ubicaciones enumeradas en la salida, la alerta Objetos perdidos podría ser un falso positivo. Confirmar 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 se encuentra en la ubicación indicada. (El procedimiento para "buscando objetos potencialmente perdidos" (Explica cómo utilizar 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 ubicaciones enumeradas en la salida, es posible que el objeto no esté presente. Puedes intentarlo "buscar y restaurar el objeto" usted mismo o puede ponerse en contacto con el soporte técnico. Es posible que el soporte técnico le pida que determine si hay un procedimiento de recuperación de almacenamiento en curso. Ver la información sobre "Restaurar datos de objetos mediante Grid Manager" y "restaurar datos de objetos a un volumen de almacenamiento".

Buscar y restaurar objetos potencialmente perdidos

Es posible que sea posible encontrar y restaurar objetos que hayan activado una alerta de **Objeto perdido** y una alarma de Objetos perdidos (LOST) heredada y que usted haya identificado como potencialmente perdidos.

Antes de empezar

- Tienes el UUID de cualquier objeto perdido, tal como se identifica en ["Investigar objetos perdidos"](#).
- Tú tienes el `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 encontrará. Sin embargo, en algunos casos, es posible que puedas encontrar y restaurar un objeto replicado perdido si tomas medidas rápidamente.



Comuníquese con el soporte técnico para obtener ayuda con este procedimiento.

Pasos

1. Desde un nodo de administración, busque en los registros de auditoría posibles ubicaciones de objetos:
 - a. Inicie sesión en el nodo de la red:
 - i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - iii. Introduzca el siguiente comando para cambiar a root: `su -`
 - iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo. Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.
 - b. Cambie al directorio donde se encuentran los registros de auditoría.

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

Opción	Destino
Nodos locales (predeterminado)	<code>/var/local/log/localaudit.log</code>
Nodos de administración/nodos locales	• Nodos de administración (principales y no principales): <code>/var/local/audit/export/audit.log</code> • Todos los nodos: El <code>/var/local/log/localaudit.log</code> En este modo, el archivo normalmente está vacío o falta.
Servidor syslog externo	<code>/var/local/log/localaudit.log</code>

Dependiendo de la configuración de destino de su auditoría, ingrese: `cd /var/local/log o /var/local/audit/export/`

Para obtener más información, consulte ["Seleccionar destinos de información de auditoría"](#).

- c. Utilice `grep` para extraer el ["mensajes de auditoría asociados con el objeto potencialmente perdido"](#) y enviarlos a un archivo de salida. Ingresar: `grep uuid-value audit_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. Ingresar: `grep LLST output_file_name`

Por ejemplo:

```
Admin: # grep LLST /var/local/tmp/messages_about_lost_objects.txt
```

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

```
[AUDT:[NOID(UI32):12448208][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD(CSTR):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA#3tN6"]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):15815351
34379225]
[ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CLSM][ATID(UI64):70
86871083190743409]]
```

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

Si está presente, el valor de PCLD es la ruta completa en el disco a la copia del objeto replicado faltante. El valor de NOID es el identificador del nodo del LDR donde se podría encontrar una copia del objeto.

Si encuentra la ubicación de un objeto, es posible que pueda restaurarlo.

a. Encuentre el nodo de almacenamiento asociado con este ID de nodo LDR. En el Administrador de cuadrícula, seleccione **SOPORTE > Herramientas > Topología de cuadrícula**. Luego seleccione **Centro de datos > Nodo de almacenamiento > LDR**.

El ID de nodo para el servicio LDR se encuentra en la tabla de información del nodo. Revise la información de cada nodo de almacenamiento hasta encontrar el que aloja este LDR.

2. Determine si el objeto existe en el nodo de almacenamiento indicado en el mensaje de auditoría:

a. Inicie sesión en el nodo de la red:

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

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

b. Determinar si existe la ruta del archivo del objeto.

Para la ruta 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'
```



Encierre siempre la ruta del archivo objeto entre comillas simples en los comandos para escapar de cualquier carácter especial.

- 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 siguiente paso. Puede intentar restaurar el objeto encontrado en StorageGRID.

3. Si se encontró la ruta del objeto, intente restaurar el objeto en StorageGRID:

- Desde el mismo nodo de almacenamiento, cambie la propiedad del archivo de objeto para que pueda ser administrado por StorageGRID. Ingresar: `chown ldr-user:bycast 'file_path_of_object'`
- Telnet al host local 1402 para acceder a la consola LDR. Ingresar: `telnet 0 1402`
- Ingresar: `cd /proc/STOR`
- Ingresar: `Object_Found 'file_path_of_object'`

Por ejemplo, introduzca:

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

Emisión de la `Object_Found` El comando notifica a la cuadrícula la ubicación del objeto. También activa las políticas ILM activas, que realizan copias adicionales según lo especificado en cada política.



Si el nodo de almacenamiento donde encontró el objeto está fuera de línea, puede copiar el objeto a cualquier nodo de almacenamiento que esté en línea. Coloque el objeto en cualquier directorio `/var/local/rangedb` del nodo de almacenamiento en línea. Luego, emita el `Object_Found` comando que utiliza esa ruta de archivo al objeto.

- Si no se puede restaurar el objeto, el `Object_Found` El comando falla. Póngase en contacto con el soporte técnico.
- Si el objeto se restauró exitosamente en StorageGRID, aparecerá 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 siguiente paso.

- Si el objeto se restauró exitosamente en StorageGRID, verifique que se hayan creado las nuevas ubicaciones:
 - Sign in en Grid Manager usando un ["navegador web compatible"](#).
 - Seleccione **ILM > Búsqueda de metadatos de objetos**.
 - Ingrese el UUID y seleccione **Buscar**.
 - Revise los metadatos y verifique las nuevas ubicaciones.

5. Desde un nodo de administración, busque en los registros de auditoría el mensaje de auditoría ORLM de este objeto para confirmar que la gestión del ciclo de vida de la información (ILM) ha colocado copias según sea necesario.
 - a. Inicie sesión en el nodo de la red:
 - i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - iii. Introduzca el siguiente comando para cambiar a root: `su -`
 - iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo. Cuando inicia sesión como root, el mensaje cambia de \$ a # .
 - b. Cambie al directorio donde se encuentran los registros de auditoría. Referirse a [subpaso 1.b](#) .
 - c. Utilice `grep` para extraer los mensajes de auditoría asociados con el objeto a un archivo de salida. Ingresar: `grep uuid-value audit_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 de reglas de objeto cumplidas (ORLM) de este archivo de salida. Ingresar: `grep ORLM output_file_name`

Por ejemplo:

```
Admin: # grep ORLM /var/local/tmp/messages_about_restored_object.txt
```

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

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

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

Si está presente, el valor de `CLDI` en `LOCS` es el ID del nodo y el ID del volumen donde se ha creado una copia del 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. ["Restablecer los recuentos de objetos perdidos y faltantes"](#) en el Administrador de cuadrícula.

Restablecer el recuento de objetos perdidos y faltantes

Después de investigar el sistema StorageGRID y verificar que todos los objetos perdidos registrados se perdieron de forma permanente o que es una falsa alarma, puede restablecer el valor del atributo Objetos perdidos a cero.

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .

Acerca de esta tarea

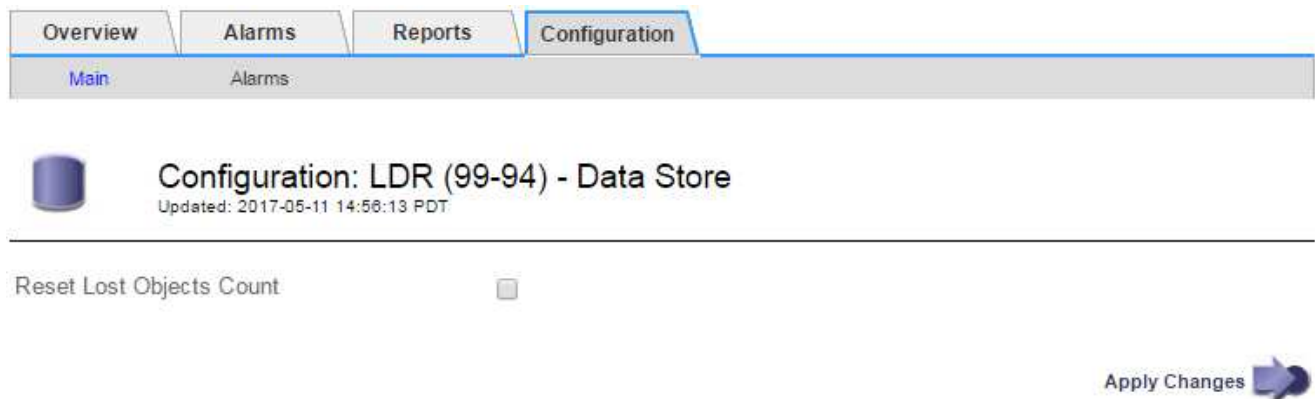
Puede restablecer el contador de objetos perdidos desde cualquiera de las siguientes páginas:

- **SOPORTE > Herramientas > Topología de cuadrícula > Sitio > Nodo de almacenamiento > LDR > Almacén de datos > Descripción general > Principal**
- **SOPORTE > Herramientas > Topología de cuadrícula > Sitio > Nodo de almacenamiento > DDS > Almacén de datos > Descripción general > Principal**

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

Pasos

1. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
2. Seleccione **Sitio > Nodo de almacenamiento > LDR > Almacén de datos > Configuración** para el nodo de almacenamiento que tiene la alerta **Objetos perdidos** o la alarma LOST.
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 PERDIDO se borran, lo que puede tardar unos minutos.

5. Opcionalmente, restablezca otros valores de atributos relacionados que podrían haberse incrementado en el proceso de identificación del objeto perdido.
 - a. Seleccione **Sitio > Nodo de almacenamiento > LDR > Codificación de borrado > Configuración**.
 - b. Seleccione **Restablecer recuento de errores de lectura y Restablecer recuento de copias corruptas detectadas**.
 - c. Haga clic en **Aplicar cambios**.

- d. Seleccione **Sitio > Nodo de almacenamiento > LDR > Verificación > Configuración**.
- e. Seleccione **Restablecer recuento de objetos faltantes 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 reemplaza automáticamente el objeto dañado y es seguro eliminar los objetos en cuarentena. Sin embargo, si se activa la alerta **Objetos perdidos** o la alarma LOST, es posible que el soporte técnico desee acceder a los objetos en cuarentena.

- g. Haga clic en **Aplicar cambios**.

Los atributos pueden tardar unos minutos en restablecerse después de hacer clic en **Aplicar cambios**.

Solucionar la alerta de almacenamiento de datos de objetos bajos

La alerta **Almacenamiento de datos de objetos bajo** monitorea 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"](#).
- Tienes ["permisos de acceso específicos"](#).

Acerca de esta tarea

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

De forma predeterminada, se activa una alerta importante cuando esta condición se evalúa como verdadera:

```
(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 datos de objetos replicados y codificados por borrado para un nodo de almacenamiento.
- ``storagegrid_storage_utilization_usable_space_bytes`` es la cantidad total de espacio de almacenamiento de objetos restante para un nodo de almacenamiento.

Si se activa una alerta mayor o menor de **Almacenamiento de datos de objetos bajo**, debe realizar un procedimiento de expansión lo antes posible.

Pasos

1. Seleccione **ALERTAS > Actual**.

Aparece la página de Alertas.

- Desde la tabla de alertas, expanda el grupo de alerta **Almacenamiento de datos de objetos bajo**, si es necesario, y seleccione la alerta que desea ver.

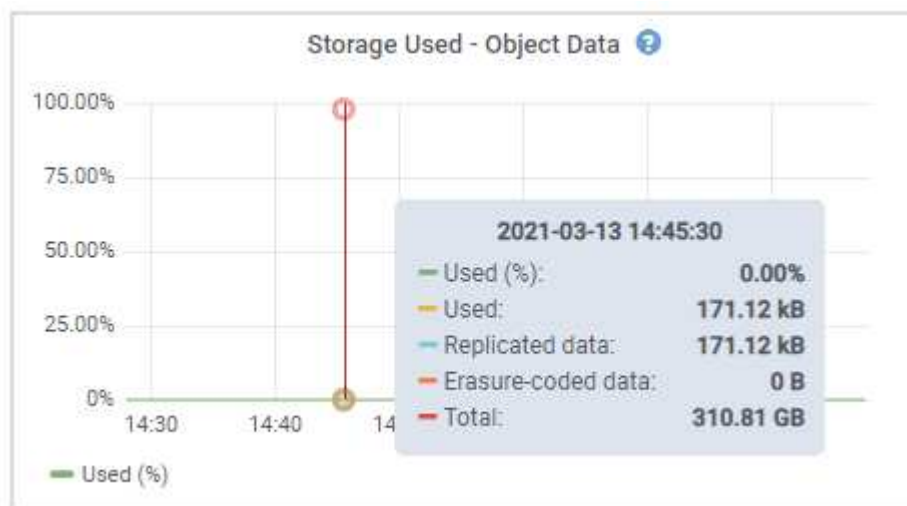


Seleccione la alerta, no el encabezado, para un grupo de alertas.

- 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 para esta alerta
- Seleccione **NODOS > Nodo de almacenamiento o Sitio > Almacenamiento**.
- Coloque el cursor sobre el gráfico Almacenamiento utilizado - Datos de objeto.

Se muestran los siguientes valores:

- **Usado (%)**: El porcentaje del espacio utilizable total que se ha utilizado para los datos del objeto.
- **Usado**: La cantidad de espacio total utilizable que se ha utilizado para los datos del objeto.
- **Datos replicados**: una estimación de la cantidad de datos de objetos replicados en este nodo, sitio o cuadrícula.
- **Datos codificados por borrado**: una 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 el `storagegrid_storage_utilization_data_bytes` métrico.



- Seleccione los controles de tiempo sobre el gráfico para ver el uso del almacenamiento en diferentes períodos de tiempo.

Mirar el uso del almacenamiento a lo largo del tiempo puede ayudarle a comprender cuánto almacenamiento se utilizó antes y después de que se activara la alerta y puede ayudarle a estimar cuánto tiempo podría tardar en llenarse el espacio restante del nodo.

- Lo antes posible, "[añadir capacidad de almacenamiento](#)" a tu red.

Puede agregar volúmenes de almacenamiento (LUN) a nodos de almacenamiento existentes o puede agregar nuevos nodos de almacenamiento.



Para obtener más información, consulte ["Administrar nodos de almacenamiento completos"](#)

Solución de problemas de alertas de anulación de marca de agua de solo lectura baja

Si utiliza valores personalizados para las marcas de agua del volumen de almacenamiento, es posible que deba resolver la alerta **Anulación de marca de agua de solo lectura baja**. Si es posible, debe actualizar su sistema para comenzar a utilizar los valores optimizados.

En versiones anteriores, los tres ["marcas de agua de volumen de almacenamiento"](#) eran configuraciones globales: los mismos valores aplicados 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, según el tamaño del nodo de almacenamiento y la capacidad relativa del volumen.

Cuando actualiza a StorageGRID 11.6 o superior, las marcas de agua optimizadas de solo lectura y lectura-escritura se aplican automáticamente a todos los volúmenes de almacenamiento, a menos que se cumpla alguna de las siguientes condiciones:

- Su sistema está cerca de su capacidad máxima y no podría aceptar nuevos datos si se aplicaran marcas de agua optimizadas. StorageGRID no cambiará la configuración de la marca de agua en este caso.
- Anteriormente ha configurado alguna de las marcas de agua del volumen de almacenamiento con un valor personalizado. StorageGRID no anulará las configuraciones de marca de agua personalizadas con valores optimizados. Sin embargo, StorageGRID puede activar la alerta **Anulación de marca de agua de solo lectura baja** si su valor personalizado para la marca de agua de solo lectura suave del volumen de almacenamiento es demasiado pequeño.

Entender la alerta

Si utiliza valores personalizados para las marcas de agua del volumen de almacenamiento, es posible que se active la alerta **Anulación de marca de agua de solo lectura baja** para uno o más nodos de almacenamiento.

Cada instancia de la alerta indica que el valor personalizado de la marca de agua de solo lectura del volumen de almacenamiento es menor que el valor mínimo optimizado para ese nodo de almacenamiento. Si continúa usando la configuración personalizada, el nodo de almacenamiento podría quedarse con muy poco espacio antes de poder pasar de forma segura al estado de solo lectura. Algunos volúmenes de almacenamiento podrían volverse inaccesibles (desmontarse automáticamente) cuando el nodo alcanza su capacidad.

Por ejemplo, supongamos que anteriormente configuró la marca de agua de solo lectura del 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 **Anulación de marca de agua de solo lectura baja** se activa para el nodo de almacenamiento A porque su marca de agua personalizada (5 GB) es más pequeña que el valor mínimo optimizado para todos los volúmenes en ese nodo (11 GB). Si continúa usando la configuración personalizada, el nodo podría quedarse con muy poco espacio antes de poder pasar de forma segura al estado de solo lectura.

Resolver la alerta

Siga estos pasos si se han activado una o más alertas de **Anulación de marca de agua de solo lectura baja**. También puede utilizar estas instrucciones si actualmente utiliza configuraciones de marca de agua personalizadas y desea comenzar a utilizar configuraciones optimizadas incluso si no se han activado alertas.

Antes de empezar

- Ha completado la actualización a StorageGRID 11.6 o superior.
- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#) .
- Tú tienes el ["Permiso de acceso root"](#) .

Acerca de esta tarea

Puede resolver la alerta **Anulación de marca de agua de solo lectura baja** actualizando las configuraciones de marca de agua personalizadas a las nuevas anulaciones de marca de agua. Sin embargo, si uno o más nodos de almacenamiento están cerca de llenarse o tiene requisitos ILM especiales, primero debe ver las marcas de agua de almacenamiento optimizadas y determinar si es seguro usarlas.

Evaluar el uso de datos de objetos para toda la red

Pasos

1. Seleccione **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 en cada sitio.

Nodes

View the list and status of sites and grid nodes.

Search... 

Total node count: 13

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID	Grid	61%	4%	—
▲ Data Center 1	Site	56%	3%	—
DC1-ADM	Primary Admin Node	—	—	6%
DC1-GW	Gateway Node	—	—	1%
! DC1-SN1	Storage Node	71%	3%	30%
! DC1-SN2	Storage Node	25%	3%	42%
! DC1-SN3	Storage Node	63%	3%	42%
! DC1-SN4	Storage Node	65%	3%	41%

4. Siga el paso apropiado:

- Si ninguno de los nodos de almacenamiento está cerca de estar lleno (por ejemplo, todos los valores de **Datos de objeto utilizados** son inferiores al 80%), puede comenzar a utilizar la configuración de anulación. Vaya a [Utilice marcas de agua optimizadas](#).
- Si las reglas de ILM utilizan un comportamiento de ingesta estricto o si los grupos de almacenamiento específicos están cerca de estar llenos, realice los pasos en [Ver marcas de agua de almacenamiento optimizadas](#) y [Determinar si puede utilizar marcas de agua optimizadas](#).

Ver marcas de agua de almacenamiento optimizadas

StorageGRID utiliza dos métricas de Prometheus para mostrar los valores optimizados que ha calculado para la marca de agua de solo lectura del volumen de almacenamiento. Puede ver los valores mínimos y máximos optimizados para cada nodo de almacenamiento en su red.

Pasos

- Seleccione **SOPORTE > Herramientas > Métricas**.
- En la sección Prometheus, seleccione el enlace para acceder a la interfaz de usuario de Prometheus.
- Para ver la marca de agua de solo lectura mínima recomendada, ingrese la siguiente métrica de Prometheus y seleccione **Ejecutar**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

La última columna muestra el valor mínimo optimizado de la marca de agua de solo lectura suave para

todos los volúmenes de almacenamiento en cada nodo de almacenamiento. Si este valor es mayor que la configuración personalizada para la marca de agua de solo lectura suave del volumen de almacenamiento, se activa la alerta **Anulación de marca de agua de solo lectura baja** para el nodo de almacenamiento.

4. Para ver la marca de agua de solo lectura suave máxima recomendada, ingrese la siguiente métrica de Prometheus y seleccione **Ejecutar**:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

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

5. Tenga en cuenta el valor máximo optimizado para cada nodo de almacenamiento.

Determinar si se pueden usar marcas de agua optimizadas

Pasos

1. Seleccione **NODOS**.
2. Repita estos pasos para cada nodo de almacenamiento en línea:
 - a. Seleccione **Nodo de almacenamiento > Almacenamiento**.
 - b. Desplácese hacia abajo hasta la tabla Almacenes de objetos.
 - c. Compare el valor **Disponible** para 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 en 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 comenzar a utilizar las marcas de agua optimizadas.

De lo contrario, amplíe la red lo antes posible. Cualquiera ["agregar volúmenes de almacenamiento"](#) a un nodo existente o ["agregar nuevos nodos de almacenamiento"](#). Luego, ve a [Utilice marcas de agua optimizadas](#) para actualizar la configuración de la marca de agua.

4. Si necesita seguir usando valores personalizados para las marcas de agua del volumen de almacenamiento, ["silencio"](#) o ["desactivar"](#) Alerta de **Anulación de marca de agua de solo lectura baja**.



Los mismos valores de marca de agua personalizados se aplican a cada volumen de almacenamiento en cada nodo de almacenamiento. El uso de valores menores a los recomendados para las marcas de agua del volumen de almacenamiento puede provocar que algunos volúmenes de almacenamiento se vuelvan inaccesibles (se desmonten automáticamente) cuando el nodo alcanza su capacidad.

Usar marcas de agua optimizadas

Pasos

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

Las configuraciones de marca de agua del volumen de almacenamiento optimizado ahora están vigentes para cada volumen de almacenamiento, según el tamaño del nodo de almacenamiento y la capacidad relativa del

volumen.

Solucionar problemas de metadatos

Si ocurren problemas con los metadatos, las alertas le informarán el origen de los problemas y las acciones recomendadas a tomar. En particular, debe agregar nuevos nodos de almacenamiento si se activa la alerta de almacenamiento de metadatos bajo.

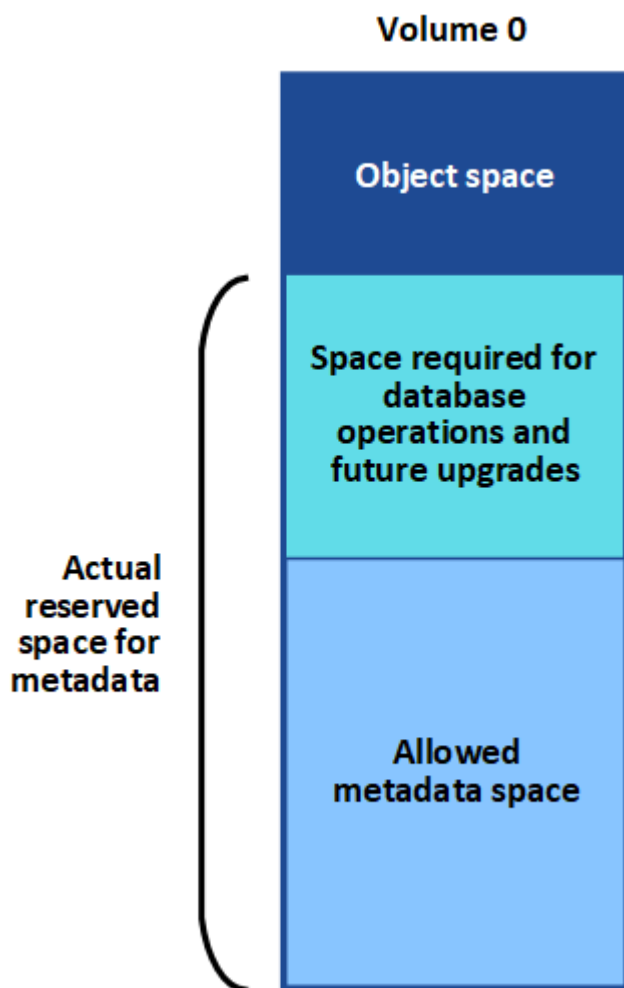
Antes de empezar

Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .

Acerca de esta tarea

Siga las acciones recomendadas para cada alerta relacionada con metadatos que se active. Si se activa la alerta **Almacenamiento de metadatos bajo**, debe agregar nuevos nodos de almacenamiento.

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



Si los metadatos de un objeto consumen más del 100% del espacio permitido para los metadatos, las operaciones de la base de datos no podrán ejecutarse de manera eficiente y se producirán errores.

Puede "[Supervisar la capacidad de metadatos de objetos para cada nodo de almacenamiento](#)" para ayudarle a anticipar errores y corregirlos antes de que ocurran.

StorageGRID utiliza la siguiente métrica de Prometheus para medir qué tan lleno está el espacio de metadatos permitido:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

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

- **Menor:** Los metadatos del objeto utilizan el 70 % o más del espacio de metadatos permitido. Debe agregar nuevos nodos de almacenamiento lo antes posible.
- **Importante:** Los metadatos del objeto están utilizando el 90 % o más del espacio de metadatos permitido. Debe agregar nuevos nodos de almacenamiento inmediatamente.



Cuando los metadatos de un objeto utilizan el 90 % o más del espacio de metadatos permitido, aparece una advertencia en el panel. Si aparece esta advertencia, debe agregar nuevos nodos de almacenamiento inmediatamente. Nunca debe permitir que los metadatos de un objeto utilicen más del 100% del espacio permitido.

- **Crítico:** Los metadatos del objeto están utilizando el 100 % o más del espacio de metadatos permitido y están comenzando a consumir el espacio necesario para las operaciones esenciales de la base de datos. Debe detener la ingesta de nuevos objetos y debe agregar nuevos nodos de almacenamiento inmediatamente.



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 para la alerta **Almacenamiento de metadatos bajo** podría ser inexacto.

Pasos

1. Seleccione **ALERTAS > Actual**.
2. Desde la tabla de alertas, expanda el grupo de alerta **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 alerta.
4. Si se ha activado una alerta importante o crítica de **Almacenamiento de metadatos bajo**, realice una expansión para agregar nodos de almacenamiento inmediatamente.



Debido a que StorageGRID mantiene copias completas de todos los metadatos de los objetos en cada sitio, la capacidad de metadatos de toda la red está limitada por la capacidad de metadatos del sitio más pequeño. Si necesita agregar capacidad de metadatos a un sitio, también debe "[ampliar cualquier otro sitio](#)" por el mismo número de nodos de almacenamiento.

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

Solucionar errores de certificado

Si observa un problema de seguridad o de certificado cuando intenta conectarse a StorageGRID mediante un navegador web, un cliente S3 o una herramienta de monitoreo externa, debe verificar el certificado.

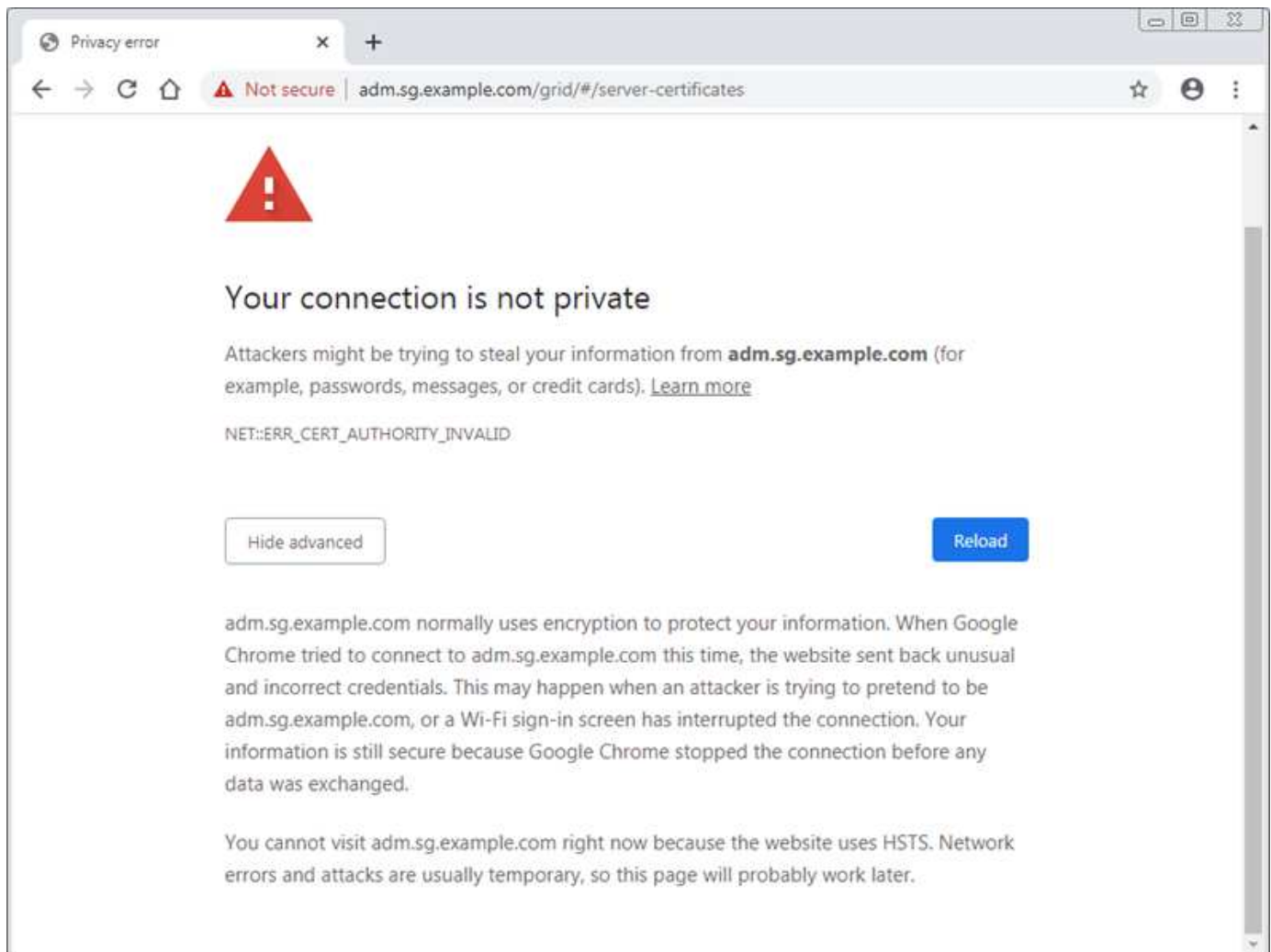
Acerca de esta tarea

Los errores de certificado pueden causar problemas cuando intenta conectarse a StorageGRID mediante Grid Manager, Grid Management API, Tenant Manager o Tenant Management API. También pueden ocurrir errores de certificado cuando intenta conectarse con un cliente S3 o una herramienta de monitoreo externa.

Si accede al Administrador de red o al Administrador de inquilinos mediante un nombre de dominio en lugar de una dirección IP, el navegador muestra un error de certificado sin una opción para omitirlo si ocurre alguna de las siguientes situaciones:

- Su certificado de interfaz de administración personalizada caduca.
- Vuelve de un certificado de interfaz de administración personalizado al certificado de servidor predeterminado.

El siguiente ejemplo muestra un error de certificado cuando el certificado de la interfaz de administración personalizada expiró:



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

Cuando utiliza certificados de cliente para la integración externa de Prometheus, los errores de certificado pueden ser causados por el certificado de la interfaz de administración de StorageGRID o por los certificados de cliente. La alerta **Expiración de certificados de cliente configurados en la página Certificados** se activa cuando un certificado de cliente está a punto de expirar.

Pasos

Si recibió una notificación de alerta sobre un certificado vencido, acceda a los detalles del certificado: . Seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego ["Seleccione la pestaña de certificado apropiada"](#) .

1. Verifique el período de validez del certificado. + Algunos navegadores web y clientes S3 no aceptan certificados con un período de validez superior a 398 días.
2. Si el certificado ha expirado o expirará pronto, cargue o genere un nuevo certificado.
 - Para obtener un certificado de servidor, consulte los pasos para ["Configuración de un certificado de servidor personalizado para Grid Manager y Tenant Manager"](#) .
 - Para obtener un certificado de cliente, consulte los pasos para ["configurar un certificado de cliente"](#) .
3. Para errores de certificado de servidor, pruebe una o ambas de las siguientes opciones:
 - Asegúrese de que el nombre alternativo del sujeto (SAN) del certificado esté completo y que el SAN coincida con la dirección IP o el nombre de host del nodo al que se está conectando.
 - Si está intentando conectarse a StorageGRID usando un nombre de dominio:
 - i. Ingrese la dirección IP del nodo de administración en lugar del nombre de dominio para evitar el error de conexión y acceder al administrador de red.
 - ii. Desde el Administrador de red, seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego ["Seleccione la pestaña de certificado apropiada"](#) 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 Grid Manager y Tenant Manager"](#) .

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

Puede realizar varias tareas para ayudar a determinar el origen de los problemas relacionados con los nodos de administración y la interfaz de usuario de StorageGRID .

Errores de inicio de sesión en el nodo de administración

Si experimenta un error al iniciar sesión en un nodo de administración de StorageGRID , es posible que su sistema tenga un problema con un ["redes"](#) o ["hardware"](#) problema, un problema con ["Servicios del nodo de administración"](#) , o un ["Problema con la base de datos de Cassandra"](#) en nodos de almacenamiento conectados.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el `Passwords.txt` archivo.

- Tienes ["permisos de acceso específicos"](#) .

Acerca de esta tarea

Utilice estas pautas de solución de problemas si ve alguno de los siguientes mensajes de error al intentar iniciar sesión en un nodo de administración:

- 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 nuevamente.

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

2. Si su sistema StorageGRID tiene más de un nodo de administración, intente iniciar sesión en Grid Manager desde otro nodo de administración para verificar el estado de un nodo de administración no disponible.
 - Si puede iniciar sesión, puede utilizar las opciones **Panel de control**, **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. Determinar si el hardware del nodo está fuera de línea.
4. Si el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID , consulte los pasos para ["configuración del inicio de sesión único"](#) .

Es posible que necesites deshabilitar y volver a habilitar temporalmente el SSO para un solo nodo de administración para resolver cualquier problema.



Si SSO está habilitado, no podrá iniciar sesión usando un puerto restringido. Debes utilizar el puerto 443.

5. Determinar si la cuenta que estás 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. Revisar alertas.
 - ii. Seleccione **CONFIGURACIÓN > Control de acceso > Federación de identidades**.
 - iii. Haga clic en **Probar conexión** para validar su 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 el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

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

7. Ver el estado de todos los servicios que se ejecutan en el nodo de la red: `storagegrid-status`

Asegúrese de que los servicios nms, mi, nginx y mgmt api estén todos en ejecución.

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

```
$ 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 esté ejecutando # `service nginx-gw status`

9. Utilice Lumberjack para recolectar troncos: `# /usr/local/sbin/lumberjack.rb`

Si la autenticación falló en el pasado, puede usar las opciones de script `--start` y `--end` de Lumberjack para especificar el rango de tiempo apropiado. Utilice `lumberjack -h` para obtener detalles sobre estas opciones.

La salida a la 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, emita cualquiera de los siguientes comandos para determinar las direcciones IP de los tres nodos de almacenamiento que ejecutan el servicio ADC en su sitio. Normalmente, estos son los primeros tres nodos de almacenamiento que se instalan en el sitio.

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

```
# gpt-list-services adc
```

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

12. Desde el nodo de administración, use `ssh` para iniciar sesión en cada uno de los nodos de almacenamiento de ADC, utilizando las direcciones IP que identificó.
13. Ver el estado de todos los servicios que se ejecutan en el nodo de la red: `storagegrid-status`

Asegúrese de que los servicios `idnt`, `acct`, `nginx` y `cassandra` estén todos en ejecución.

14. Repetir los pasos [Utilice a Lumberjack para recolectar troncos](#) y [Revisar registros](#) para revisar los registros en los nodos de almacenamiento.
15. Si no puede resolver el problema, comuníquese con el soporte técnico.

Proporcione los registros que recopiló al soporte técnico. Consulte también ["Referencia de archivos de registro"](#).

Problemas de interfaz de usuario

Es posible que la interfaz de usuario del Administrador de red o del Administrador de inquilinos no responda como se espera después de actualizar el software StorageGRID.

Pasos

1. Asegúrate de que estás usando un ["navegador web compatible"](#).
2. Limpia el caché de tu navegador web.

Al borrar la memoria 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.

Solucionar problemas de red, hardware y plataforma

Hay 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 "422: Entidad no procesable"

El error 422: Entidad no procesable puede ocurrir por diferentes motivos. Verifique el mensaje de error para determinar qué causó el problema.

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

Mensaje de error	Causa raíz y acción correctiva
<pre>422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839</pre>	Este mensaje puede aparecer si selecciona la opción No usar TLS para Seguridad de la capa de transporte (TLS) al configurar la federación de identidad mediante Windows Active Directory (AD). El uso de la opción No usar TLS no es compatible con servidores AD que implementan la firma LDAP. Debe seleccionar la opción Usar STARTTLS o la opción Usar LDAPS para TLS.

Mensaje de error	Causa raíz y acción correctiva
<pre>422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)</pre>	Este mensaje aparece si intenta utilizar un cifrado no compatible para realizar una conexión de seguridad de la capa de transporte (TLS) desde StorageGRID a un sistema externo utilizado para identificar federaciones o grupos de almacenamiento en la nube. Verifique los cifrados 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 la red Grid

La alerta **Desajuste de MTU de red de cuadrícula** se activa cuando la configuración de la unidad de transmisión máxima (MTU) para la interfaz de red de cuadrícula (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. Una discrepancia en el tamaño de MTU de más de 1000 podría provocar problemas de rendimiento de la red.

Pasos

1. Enumere las configuraciones de MTU para eth0 en todos los nodos.
 - Utilice la consulta proporcionada en el Administrador de cuadrícula.
 - Navegar a *primary Admin Node IP address/metrics/graph* e ingrese la siguiente consulta: `node_network_mtu_bytes{device="eth0"}`
2. ["Modificar la configuración de MTU"](#) según sea necesario para garantizar que sean los mismos para la interfaz de red Grid (eth0) en todos los nodos.
 - Para los nodos basados en Linux y VMware, utilice 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 excede 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 usar el `change-ip.py` script para cambiar el valor de MTU de la red en el contenedor.

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

Argumentos posicionales	Descripción
<code>mtu</code>	La MTU a configurar. Debe estar en el rango de 1280 a 9216.
<code>network</code>	Las redes a las que se aplicará la MTU. Incluya uno o más de los siguientes tipos de red: • red • administración • cliente

+

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

Alerta de error en la recepción de trama de la red del nodo

Las alertas de **Error de trama de recepción de red de nodo** pueden deberse a problemas de conectividad entre StorageGRID y el hardware de su red. Esta alerta desaparece por sí sola una vez que se soluciona el problema subyacente.

Acerca de esta tarea

Las alertas de **Error de trama de recepción de red de nodo** pueden deberse a los siguientes problemas con el hardware de red que se conecta a StorageGRID:

- La corrección de errores hacia adelante (FEC) es necesaria y no se utiliza
- Desajuste entre el puerto del conmutador y la MTU de la NIC
- Altas tasas de error de enlace
- Desbordamiento del búfer de anillo de la NIC

Pasos

1. Siga los pasos de solución de problemas para todas las posibles causas de esta alerta dada su configuración de red.
2. Realice los siguientes pasos según la causa del error:

Desajuste de FEC



Estos pasos se aplican únicamente a las alertas de **Error de trama de recepción de red de nodo** provocadas por una falta de coincidencia de FEC en los dispositivos StorageGRID .

- a. Verifique el estado FEC del puerto en el conmutador conectado a su dispositivo StorageGRID .
- b. Verifique la integridad física de los cables del aparato al interruptor.
- c. Si desea cambiar la configuración de FEC para intentar resolver la alerta, primero asegúrese de que el dispositivo esté configurado para el modo **Automático** en la página Configuración de enlace del Instalador del dispositivo StorageGRID (consulte las instrucciones para su dispositivo):
 - "SG6160"
 - "SGF6112"
 - "SG6000"
 - "SG5800"
 - "SG5700"
 - "SG110 y SG1100"
 - "SG100 y SG1000"
- d. Cambie la configuración de FEC en los puertos del conmutador. Los puertos del dispositivo StorageGRID ajustarán su configuración FEC para que coincida, si es posible.

No se pueden configurar los ajustes de FEC en los dispositivos StorageGRID . En lugar de ello, los dispositivos intentan descubrir y reflejar la configuración de FEC en los puertos del conmutador a los que están conectados. Si los enlaces se fuerzan a velocidades de red de 25 GbE o 100 GbE, es posible que el conmutador y la NIC no puedan negociar una configuración FEC común. Sin una configuración FEC común, la red volverá al modo "sin FEC". Cuando FEC no está habilitado, las conexiones son más susceptibles a errores causados por ruido eléctrico.



Los dispositivos StorageGRID admiten FEC Firecode (FC) y Reed Solomon (RS), así como también no admiten FEC.

Desajuste entre el puerto del conmutador y la MTU de la NIC

Si la alerta es causada por una falta de coincidencia entre el puerto del conmutador y la MTU de la NIC, verifique que el tamaño de MTU configurado en el nodo sea el mismo que la configuración de MTU para el puerto del conmutador.

El tamaño de MTU configurado en el nodo puede ser menor que la configuración en el puerto del conmutador al que está conectado el nodo. Si un nodo StorageGRID recibe una trama Ethernet más grande que su MTU, lo cual es posible con esta configuración, es posible que se informe la alerta **Error de trama de recepción de red de nodo**. Si cree que esto es lo que está sucediendo, cambie la MTU del puerto del conmutador para que coincida con la MTU de la interfaz de red StorageGRID , o cambie la MTU de la interfaz de red StorageGRID para que coincida con el puerto del conmutador, según sus objetivos o requisitos de MTU de extremo a extremo.



Para obtener el mejor rendimiento de la red, todos los nodos deben configurarse con valores de MTU similares en sus interfaces de red Grid. La alerta **No coincide la MTU de la red de cuadrícula** se activa si hay una diferencia significativa en las configuraciones de MTU para la red de cuadrícula en nodos individuales. Los valores de MTU no tienen que ser los mismos para todos los tipos de red. Ver [Solucionar la alerta de desajuste de MTU de la red Grid](#) Para más información.



Ver también "[Cambiar la configuración de MTU](#)".

Altas tasas de error de enlace

- Habilitar FEC, si aún no está habilitado.
- Verifique que su cableado de red sea de buena calidad y no esté dañado o mal conectado.
- Si los cables no parecen ser el problema, comuníquese con el soporte técnico.



Es posible que notes altos índices de error en un entorno con alto ruido eléctrico.

Desbordamiento del búfer de anillo de la NIC

Si el error es un desbordamiento del búfer del anillo de NIC, comuníquese con el soporte técnico.

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

- Monitoree el problema y comuníquese con el soporte técnico si la alerta no se resuelve.

Errores de sincronización horaria

Es posible que experimente problemas con la sincronización horaria en su red.

Si encuentra problemas de sincronización horaria, verifique que haya especificado al menos cuatro fuentes NTP externas, cada una de las cuales proporcione una referencia Stratum 3 o superior, y que todas las fuentes NTP externas estén funcionando normalmente y sean accesibles para los nodos StorageGRID.



Cuando "[especificando la fuente NTP externa](#)" Para una instalación de StorageGRID a nivel de producción, no utilice el servicio de hora de Windows (W32Time) en una versión de Windows anterior a Windows Server 2016. El servicio de hora en versiones anteriores de Windows no es lo suficientemente preciso y Microsoft no lo admite para su uso en entornos de alta precisión, como StorageGRID.

Linux: Problemas de conectividad de red

Es posible que experimente problemas con la conectividad de red para los nodos 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 está utilizando hosts virtuales, configure el valor de la clave de clonación de dirección MAC para cada una de sus redes en "verdadero" en su archivo de configuración de nodo. Esta configuración hace que la dirección MAC del contenedor StorageGRID utilice la dirección MAC del host. Para crear archivos de configuración de

nodo, consulte las instrucciones para ["Red Hat Enterprise Linux"](#) o ["Ubuntu o Debian"](#) .



Cree interfaces de red virtuales independientes para que las utilice el sistema operativo host Linux. El uso de las mismas interfaces de red para el sistema operativo host Linux y el contenedor StorageGRID puede provocar que el sistema operativo host se vuelva inaccesible si no se ha habilitado el modo promiscuo en el hipervisor.

Para obtener más información sobre cómo habilitar la clonación de MAC, consulte las instrucciones para ["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 configuradas en **Aceptar** para Modo promiscuo, Cambios de dirección MAC y Transmisiones falsificadas. Los valores establecidos en el conmutador virtual pueden ser anulados por los valores a nivel del grupo de puertos, así que asegúrese de que las configuraciones sean las mismas en ambos lugares.

Para obtener más información sobre el uso del modo promiscuo, consulte las instrucciones para ["Red Hat Enterprise Linux"](#) o ["Ubuntu o Debian"](#) .

Linux: El estado del nodo es "huérfano"

Un nodo Linux en estado huérfano generalmente indica que el servicio StorageGrid o el demonio del nodo StorageGRID que controla el contenedor del nodo murió inesperadamente.

Acerca de esta tarea

Si un nodo Linux informa que está en estado huérfano, debe:

- Verifique los registros para detectar errores y mensajes.
- Intente iniciar el nodo nuevamente.
- Si es necesario, utilice los comandos del motor de contenedor para detener el contenedor de nodo existente.
- Reinicie el nodo.

Pasos

1. Verifique los registros tanto del demonio de servicio como del nodo huérfano para detectar errores obvios o mensajes sobre salidas inesperadas.
2. Inicie sesión en el host como root o usando una cuenta con permiso sudo.
3. Intente iniciar el nodo nuevamente 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 del contenedor y cualquier proceso de control del nodo de almacenamiento en red. Por ejemplo: `sudo docker stop --time secondscontainer-name`

Para `seconds`, ingrese la cantidad de segundos que desea esperar hasta que el contenedor se detenga (normalmente 15 minutos o menos). Por ejemplo:

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

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

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

Linux: Solución de problemas de compatibilidad con IPv6

Es posible que necesite habilitar la compatibilidad con IPv6 en el kernel si ha instalado nodos StorageGRID en hosts Linux y observa que las direcciones IPv6 no se han asignado a los contenedores de nodos como se esperaba.

Acerca de esta tarea

Para ver la dirección IPv6 que se ha asignado a un nodo de la red:

1. Seleccione **NODOS** y seleccione el nodo.
2. Seleccione **Mostrar direcciones IP adicionales** junto a **Direcciones IP** en la pestaña Descripción general.

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

Pasos

1. Inicie sesión en el host como root o usando 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 de su sistema operativo para cambiarlo. `sysctl` ajustes. Luego, cambie el valor a 0 antes de continuar.

3. Ingrese al contenedor del 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. Salir del contenedor: `exit`

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

6. Como root, 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 siguientes dos líneas y elimine las etiquetas de comentarios. Luego, 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 StorageGRID :

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

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

Solucionar problemas de un servidor syslog externo

La siguiente tabla describe los mensajes de error que pueden estar relacionados con el uso de un servidor syslog externo y enumera 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 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 cómo enviar información de auditoría a un servidor syslog externo, consulte:

- "[Consideraciones para el uso de un servidor syslog externo](#)"
- "[Configurar mensajes de auditoría y servidor syslog externo](#)"

Mensaje de error	Descripción y acciones recomendadas
No se puede resolver el nombre de host	El FQDN que ingresó para el servidor syslog no se pudo resolver a una dirección IP. 1. Verifique el nombre de host ingresado. Si ingresó una dirección IP, asegúrese de que sea una dirección IP válida en notación WXYZ ("decimal punteado"). 2. Verifique que los servidores DNS estén configurados correctamente. 3. Confirme que cada nodo pueda acceder a las direcciones IP del servidor DNS.
Conexión rechazada	Se rechazó una conexión TCP o TLS al servidor syslog. Es posible que no haya ningún servicio escuchando en el puerto TCP o TLS del host, o que un firewall esté bloqueando el acceso. 1. Verifique que haya ingresado el FQDN o la dirección IP, el puerto y el protocolo correctos para el servidor syslog. 2. Confirme que el host del servicio syslog esté ejecutando un demonio syslog que esté escuchando en el puerto especificado. 3. Confirme que un firewall no esté bloqueando el acceso a las conexiones TCP/TLS desde los nodos a la IP y al puerto del servidor syslog.
Red inalcanzable	El servidor syslog no está en una subred conectada directamente. Un enrutador devolvió un mensaje de error ICMP para indicar que no pudo reenviar los mensajes de prueba desde los nodos enumerados al servidor syslog. 1. Verifique que haya ingresado el FQDN o la dirección IP correctos para el servidor syslog. 2. Para cada nodo enumerado, verifique la Lista de subredes de red de cuadrícula, las Listas de subredes de redes de administración y las puertas de enlace de red de cliente. Confirme que estén configurados para enrutar el tráfico al servidor 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 inalcanzable	El servidor syslog está en una subred conectada directamente (subred utilizada por los nodos enumerados para sus direcciones IP de red, 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. Verifique que haya ingresado el FQDN o la dirección IP correctos para el servidor syslog. 2. Compruebe que el host que ejecuta el servicio syslog esté activo.
Se agotó el tiempo de conexión	Se intentó una conexión TCP/TLS, pero no se recibió respuesta del servidor syslog durante mucho tiempo. Es posible que haya una configuración incorrecta de enrutamiento o que un firewall esté descartando tráfico sin enviar ninguna respuesta (una configuración común). 1. Verifique que haya ingresado el FQDN o la dirección IP correctos para el servidor syslog. 2. Para cada nodo enumerado, verifique la Lista de subredes de red de cuadrícula, las Listas de subredes de redes de administración y las puertas de enlace de red de cliente. Confirme que estén configurados para enrutar el tráfico al servidor syslog utilizando la interfaz de red y la puerta de enlace (Grid, Admin o Cliente) a través de las cuales espera que se llegue al servidor syslog. 3. Confirme que un firewall no esté bloqueando el acceso a las conexiones TCP/TLS desde los nodos enumerados a la IP y al puerto del servidor syslog.
Conexión cerrada por el socio	Se estableció exitosamente una conexión TCP con el servidor syslog pero luego se cerró. Las razones para esto podrían incluir: • Es posible que se haya reiniciado o reiniciado el servidor syslog. • El nodo y el servidor syslog pueden tener diferentes configuraciones TCP/TLS. • Es posible que un firewall intermedio esté cerrando conexiones TCP inactivas. • Es posible que un servidor que no sea syslog y que esté escuchando en el puerto del servidor syslog haya cerrado la conexión. Para resolver este problema: 1. Verifique que haya ingresado el FQDN o la dirección IP, el puerto y el protocolo correctos para el servidor syslog. 2. Si está utilizando TLS, confirme que el servidor syslog también esté utilizando TLS. Si está utilizando TCP, confirme que el servidor syslog también esté utilizando TCP. 3. Compruebe que no haya un firewall intermedio configurado para cerrar conexiones TCP inactivas.

Mensaje de error	Descripción y acciones recomendadas
Error de certificado TLS	El certificado de servidor recibido del servidor syslog no era compatible con el paquete de certificados CA y el certificado de cliente que proporcionó. 1. Confirme que el paquete de certificados de CA y el certificado de cliente (si hay alguno) sean compatibles con el certificado del servidor en el servidor syslog. 2. Confirme que las identidades en el certificado del servidor del servidor syslog incluyan los valores de IP o FQDN esperados.
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 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. Verifique que haya ingresado el FQDN o la dirección IP, el puerto y el protocolo correctos para el servidor syslog. 3. Si está utilizando TLS, confirme que el servidor syslog también esté utilizando TLS. Si está utilizando TCP, confirme que el servidor syslog también esté utilizando TCP. 4. Confirme que el paquete de certificados de CA y el certificado de cliente (si hay alguno) sean compatibles con el certificado del servidor del servidor syslog. 5. Confirme que las identidades en el certificado del servidor del servidor syslog incluyan los valores de IP o FQDN esperados.
Consulta de resultados fallida	El nodo de administración utilizado para la configuración y prueba del servidor syslog no puede solicitar resultados de pruebas de los nodos enumerados. Es posible que uno o más nodos estén 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 funcionando. 2. Reinicie el servicio miscd en los nodos enumerados.

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.