



Supervisión y solución de problemas

StorageGRID software

NetApp

February 12, 2026

Tabla de contenidos

| | |
|---|-----|
| Supervisar y solucionar problemas de un sistema StorageGRID | 1 |
| Supervise el sistema StorageGRID | 1 |
| Supervisar un sistema StorageGRID | 1 |
| Permite ver y gestionar el panel de control | 1 |
| Vea la página Nodes | 4 |
| Información para monitorear regularmente | 36 |
| Gestionar alertas | 66 |
| Referencia de archivos de registro | 105 |
| Configurar la gestión de registros y el servidor syslog externo | 124 |
| Usar supervisión de SNMP | 139 |
| Recopilación de datos de StorageGRID adicionales | 151 |
| Solucionar los problemas del sistema StorageGRID | 165 |
| Solucionar los problemas de un sistema StorageGRID | 165 |
| Solucione problemas de almacenamiento y objetos | 172 |
| Solucionar problemas de metadatos | 191 |
| Solucionar errores de certificado | 193 |
| Solucione problemas del nodo de administrador y de la interfaz de usuario | 194 |
| Solucionar problemas de red, hardware y plataforma | 198 |
| Solucione problemas de un servidor de syslog externo | 205 |
| Solucionar problemas de almacenamiento en caché del balanceador de carga | 208 |
| Revisar los registros de auditoría | 209 |
| Registros y mensajes de auditoría | 209 |
| Auditar el flujo y la retención de mensajes | 210 |
| Acceda al archivo de registro de auditoría | 213 |
| Rotación del archivo de registro de auditoría | 214 |
| Formato del archivo de registro de auditoría | 214 |
| Formato de mensaje de auditoría | 227 |
| Auditar los mensajes y el ciclo de vida del objeto | 231 |
| Auditar mensajes | 238 |

Supervisar y solucionar problemas de un sistema StorageGRID

Supervise el sistema StorageGRID

Supervisar un sistema StorageGRID

Supervise su sistema StorageGRID con regularidad para garantizar que funciona como se espera.

Antes de empezar

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



Para cambiar las unidades de los valores de almacenamiento que se muestran en Grid Manager, seleccione el menú desplegable de usuario en la parte superior derecha del Grid Manager y, a continuación, seleccione **Preferencias de usuario**.

Acerca de esta tarea

Estas instrucciones describen cómo:

- "[Permite ver y gestionar el panel de control](#)"
- "[Vea la página Nodes](#)"
- "[Supervise estos aspectos del sistema regularmente:](#)"
 - "[Estado del sistema](#)"
 - "[Capacidad de almacenamiento](#)"
 - "[Gestión de la vida útil de la información](#)"
 - "[Redes y recursos del sistema](#)"
 - "[Actividad de inquilino](#)"
 - "[Operaciones de equilibrio de carga](#)"
 - "[Conexiones de federación de grid](#)"
- "[Gestionar alertas](#)"
- "[Ver archivos de registro](#)"
- "[Configurar la gestión de registros y el servidor syslog externo](#)"
- "[Use un servidor de syslog externo](#)" para recopilar información de auditoría
- "[Utilice SNMP para la supervisión](#)"
- "[Cambiar la priorización de E/S](#)" para cambiar las prioridades relativas para las operaciones de E/S

Permite ver y gestionar el panel de control

Puede utilizar la consola para supervisar las actividades del sistema de un vistazo. Puedes crear paneles personalizados para supervisar la implementación de

StorageGRID.



Para cambiar las unidades de los valores de almacenamiento que se muestran en Grid Manager, seleccione el menú desplegable de usuario en la parte superior derecha del Grid Manager y, a continuación, seleccione **Preferencias de usuario**.

La consola puede variar en función de la configuración del sistema.

The screenshot shows the StorageGRID dashboard with the following sections:

- Health status**: Shows 1 license issue (orange exclamation mark icon).
- Data space usage breakdown**: Shows 2.11 MB (0%) of 3.09 TB used overall across three Data Centers (Data Center 2, Data Center 3, Data Center 1).
- Total objects in the grid**: Shows 0 total objects.
- Metadata allowed space usage breakdown**: Shows 3.62 MB (0%) of 25.76 GB used in Data Center 1, with Data Center 1 having the highest metadata space usage.

Vea la consola

La consola consta de pestañas que contienen información específica sobre el sistema StorageGRID. Cada ficha contiene categorías de información que se muestran en las tarjetas.

Puede utilizar la consola proporcionada por el sistema tal cual. Además, puede crear paneles de control personalizados que contengan solo las pestañas y tarjetas relevantes para supervisar la implementación de StorageGRID.

Las fichas del panel de control proporcionadas por el sistema contienen tarjetas con los siguientes tipos de información:

| En la consola proporcionada por el sistema | Contiene |
|--|--|
| Descripción general | Información general sobre la cuadrícula, como alertas activas, uso del espacio y objetos totales en la cuadrícula. |
| Rendimiento | Uso de espacio, almacenamiento utilizado a lo largo del tiempo, S3 operaciones, duración de la solicitud, tasa de error. |
| Reducida | Uso de la cuota del inquilino y el uso del espacio lógico. Previsiones de uso del espacio para los datos de usuario y metadatos. |
| ILM | Cola de gestión del ciclo de vida de la información y tasa de evaluación. |
| Nodos | Uso de la CPU, los datos y la memoria por nodo. S3 operaciones por nodo. Distribución de nodo a sitio. |

Algunas de las tarjetas se pueden maximizar para facilitar la visualización. Seleccione el icono Maximizar  en la esquina superior derecha de la tarjeta. Para cerrar una tarjeta maximizada, selecciona el icono Minimizar  o selecciona **Cerrar**.

Gestionar paneles

Si dispone de acceso root (consulte "[Permisos de grupo de administradores](#)"), puede realizar las siguientes tareas de gestión para los paneles de control:

- Cree un panel de control personalizado desde cero. Puede utilizar paneles personalizados para controlar qué información de StorageGRID se muestra y cómo se organiza dicha información.
- Clonar un panel de control para crear paneles personalizados.
- Definir un panel de control activo para un usuario. La consola activa puede ser la consola proporcionada por el sistema o una consola personalizada.
- Establezca un panel de control predeterminado, que es lo que ven todos los usuarios a menos que activen su propio panel de control.
- Editar un nombre de panel de control.
- Edite un panel de control para agregar o eliminar pestañas y tarjetas. Puede tener un mínimo de 1 y un máximo de 20 pestañas.
- Eliminar un panel de control.



Si tiene cualquier otro permiso además del acceso root, solo puede establecer un panel de control activo.

Para administrar paneles, selecciona **Acciones > Administrar paneles**.

The screenshot shows the StorageGRID dashboard interface. At the top right, there is a blue 'Actions' button with a dropdown arrow. Below it, two options are highlighted with green outlines: 'Clone active dashboard' and 'Manage dashboards'. The main navigation bar at the bottom has tabs for 'Overview', 'Performance', 'Storage', 'ILM', and 'Nodes', with 'Overview' currently selected.

Configurar paneles de control

Para crear un nuevo panel clonando el panel activo, seleccione **Acciones > Clonar panel activo**.

Para editar o clonar un panel de control existente, selecciona **Acciones > Administrar paneles**.



El panel proporcionado por el sistema no se puede editar ni eliminar.

Al configurar un panel de control, puede:

- Agregar o eliminar pestañas
- Cambie el nombre de las pestañas y asigne nombres únicos a las nuevas pestañas
- Agregue, elimine o reorganice (arrastre) tarjetas para cada pestaña
- Seleccione el tamaño de las tarjetas individuales seleccionando **S, M, L o XL** en la parte superior de la tarjeta

The screenshot shows the 'Configure dashboard' interface. At the top, there is a toolbar with tabs for 'Overview', 'Performance', 'Storage', 'ILM', 'Nodes', and a '+ Add tab' button. Below the toolbar, there is a 'Tab name' input field containing 'Overview'. Underneath, there is a 'Select cards' button. The main area is divided into two sections: 'S M L' and 'M L XL'. The 'S M L' section contains a 'Health status' card with a yellow warning icon and the number '1'. The 'M L XL' section contains a 'Data space usage breakdown' card with a table showing storage usage for three Data Centers:

| Site name | Data storage usage | Used space | Total space |
|---------------|--------------------|------------|-------------|
| Data Center 1 | 0% | 1.79 MB | 1.24 TB |
| Data Center 2 | 0% | 921.11 KB | 926.62 GB |
| Data Center 3 | 0% | 790.21 KB | 926.62 GB |

Vea la página Nodes

Vea la página Nodes

Cuando necesite información más detallada sobre el sistema de StorageGRID que la que

proporciona la consola, se puede usar la página Nodos para ver métricas de todo el grid, cada sitio del grid y cada nodo de un sitio.

En la tabla Nodos, se muestra información de resumen de toda la cuadrícula, cada sitio y cada nodo. Si un nodo está desconectado o tiene una alerta activa, aparece un ícono junto al nombre del nodo. Si el nodo está conectado y no tiene alertas activas, no se muestra ningún ícono.

- i Cuando un nodo no está conectado a la cuadrícula, como durante la actualización o un estado desconectado, es posible que algunas métricas no estén disponibles o se excluyan de los totales de la ubicación y la cuadrícula. Después de que un nodo se vuelva a conectar a la cuadrícula, espere varios minutos para que los valores se stabilicen.
- i Para cambiar las unidades de los valores de almacenamiento que se muestran en Grid Manager, seleccione el menú desplegable de usuario en la parte superior derecha del Grid Manager y, a continuación, seleccione **Preferencias de usuario**.
- i Las capturas de pantalla mostradas son ejemplos. Los resultados pueden variar en función de la versión de StorageGRID.

Nodes

View the list and status of sites and grid nodes.

| Name | Type | Object data used | Object metadata used | CPU usage |
|---------------------------------|--------------------|------------------|----------------------|-----------|
| StorageGRID Webscale Deployment | Grid | 0% | 0% | — |
| DC1 | Site | 0% | 0% | — |
| ✖ DC1-ADM1 | Primary Admin Node | — | — | 6% |
| ⚠ DC1-ARC1 | Archive Node | — | — | 1% |
| ⚠ DC1-G1 | Gateway Node | — | — | 3% |
| DC1-S1 | Storage Node | 0% | 0% | 6% |
| DC1-S2 | Storage Node | 0% | 0% | 8% |
| DC1-S3 | Storage Node | 0% | 0% | 4% |

Iconos de estado de conexión

Si un nodo está desconectado de la cuadrícula, aparece cualquiera de los siguientes iconos junto al nombre del nodo.

| | Descripción | Acción necesaria |
|--|--|---|
| | <p>No conectado - Desconocido</p> <p>Por una razón desconocida, un nodo está desconectado o los servicios del nodo se desactivan inesperadamente. Por ejemplo, un servicio del nodo podría estar detenido o podría haber perdido la conexión de red debido a un fallo de alimentación o a un corte inesperado.</p> <p>La alerta no se puede comunicar con el nodo también puede activarse. Otras alertas también pueden estar activas.</p> | <p>Requiere atención inmediata. "Seleccione cada alerta" y siga las acciones recomendadas.</p> <p>Por ejemplo, es posible que deba reiniciar un servicio que haya detenido o reiniciar el host del nodo.</p> <p>Nota: Un nodo puede aparecer como Desconocido durante las operaciones de cierre administradas. Puede ignorar el estado Desconocido en estos casos.</p> |
| | <p>No conectado - administrativamente abajo</p> <p>Por un motivo esperado, el nodo no está conectado a la cuadrícula.</p> <p>Por ejemplo, el nodo o los servicios del nodo se han apagado correctamente, el nodo se está reiniciando o se está actualizando el software. Una o más alertas también pueden estar activas.</p> <p>En función del problema subyacente, estos nodos suelen volver a estar en línea sin ninguna intervención.</p> | <p>Determine si alguna alerta afecta a este nodo.</p> <p>Si hay una o más alertas activas, "Seleccione cada alerta" siga las acciones recomendadas.</p> |

Si un nodo está desconectado de la cuadrícula, puede tener una alerta subyacente, pero solo aparecerá el icono «No conectado». Para ver las alertas activas de un nodo, seleccione el nodo.

Iconos de alerta

Si hay una alerta activa de un nodo, aparece uno de los siguientes iconos junto al nombre del nodo:

Crítico: Existe una condición anormal que ha detenido las operaciones normales de un nodo o servicio StorageGRID. Debe abordar el problema subyacente de inmediato. Se pueden producir interrupciones del servicio y pérdida de datos si no se resuelve el problema.

Mayor: Existe una condición anormal que está afectando las operaciones actuales o acercándose al umbral de una alerta crítica. Debe investigar las alertas principales y solucionar cualquier problema subyacente para garantizar que esta condición no detenga el funcionamiento normal de un nodo o servicio de StorageGRID.

Menor: El sistema funciona normalmente, pero existe una condición anormal que podría afectar la capacidad del sistema para funcionar si continúa. Debe supervisar y resolver alertas menores que no borren por sí solas para asegurarse de que no den lugar a un problema más grave.

Vea detalles de un sistema, sitio o nodo

Para filtrar la información que se muestra en la tabla de nodos, introduzca una cadena de búsqueda en el campo **Search**. Puede buscar por nombre de sistema, nombre mostrado o tipo (por ejemplo, introduzca **gat** para localizar rápidamente todos los nodos de Gateway).

Para ver la información de la cuadrícula, el sitio o el nodo:

- Seleccione el nombre de la cuadrícula para ver un resumen de las estadísticas de todo el sistema StorageGRID.
- Seleccione un sitio de centro de datos específico para ver un resumen de las estadísticas de todos los nodos de ese sitio.
- Seleccione un nodo concreto para ver información detallada de ese nodo.

Vea la ficha Descripción general

La pestaña Overview proporciona información básica sobre cada nodo. También muestra todas las alertas que actualmente afectan al nodo.

La pestaña Overview se muestra para todos los nodos.

Información del nodo

La sección Información de Nodo del separador Visión General muestra información básica sobre el nodo.

NYC-ADM1 (Primary Admin Node)

Overview **Hardware** Network Storage Load balancer Tasks

Node information

| | |
|-------------------|--|
| Display name: | NYC-ADM1 |
| System name: | DC1-ADM1 |
| Type: | Primary Admin Node |
| ID: | 3adb1aa8-9c7a-4901-8074-47054aa06ae6 |
| Connection state: |  Connected |
| Software version: | 11.7.0 |
| IP addresses: | 10.96.105.85 - eth0 (Grid Network) |
| | Show additional IP addresses  |

La información general de un nodo incluye lo siguiente:

- **Nombre para mostrar** (solo se muestra si el nodo ha sido renombrado): El nombre para mostrar actual para el nodo. Utilice el "[Cambio el nombre de cuadrícula, sitios y nodos](#)" procedimiento para actualizar este valor.
- **Nombre del sistema**: El nombre que ingresó para el nodo durante la instalación. Los nombres del sistema se utilizan para operaciones internas de StorageGRID y no se pueden cambiar.
- **Tipo**: El tipo de nodo — Nodo de administración, Nodo de administración principal, Nodo de almacenamiento o Nodo de puerta de enlace.
- **ID**: Identificador único del nodo, que también se conoce como UUID.
- **Estado de conexión**: Uno de los tres estados. Se muestra el icono del estado más grave.
 - **Desconocido** : Por una razón desconocida, el nodo no está conectado a la red, o uno o más servicios están inesperadamente apagados. Por ejemplo, se ha perdido la conexión de red entre los nodos, está desconectada o un servicio está inactivo. La alerta **no se puede comunicar con el nodo** también puede activarse. Es posible que otras alertas estén activas también. Esta situación requiere atención inmediata.
 - Es posible que un nodo aparezca como desconocido durante las operaciones de apagado gestionadas. Puede ignorar el estado Desconocido en estos casos.
 - **Administrativamente abajo** : El nodo no está conectado a la red por una razón esperada. Por ejemplo, el nodo o los servicios del nodo se han apagado correctamente, el nodo se está reiniciando o se está actualizando el software. Una o más alertas también pueden estar activas.
 - **Conectado** : El nodo está conectado a la red.
- **Almacenamiento utilizado**: Sólo para nodos de almacenamiento.
 - **Datos del objeto**: Porcentaje del espacio útil total para los datos del objeto que se han utilizado en el nodo de almacenamiento.
 - **Metadatos de objetos**: Porcentaje del espacio total permitido para metadatos de objetos que se ha utilizado en el nodo de almacenamiento.
- **Versión de software**: Versión de StorageGRID instalada en el nodo.
- **Grupos de alta disponibilidad**: Sólo para nodos de nodo de administración y de puerta de enlace. Se muestra si se incluye una interfaz de red en el nodo en un grupo de alta disponibilidad y si esa interfaz es la interfaz principal.
- **Direcciones IP**: Las direcciones IP del nodo. Haga clic en **Mostrar direcciones IP adicionales** para ver las direcciones IPv4 e IPv6 y las asignaciones de interfaces del nodo.

Alertas

La sección Alertas del separador Visión General muestra cualquier "[las alertas que afectan actualmente a este nodo que no se han silenciado](#)". Seleccione el nombre de la alerta para ver detalles adicionales y acciones recomendadas.

Alerts

| Alert name | Severity | Time triggered | Current values |
|---|----------|--------------------------------|-------------------------|
| Low installed node memory 🔗 | Critical | 11 hours ago 🔗 | Total RAM size: 8.37 GB |

The amount of installed memory on a node is low.

También se incluyen alertas para "estados de conexión de nodo".

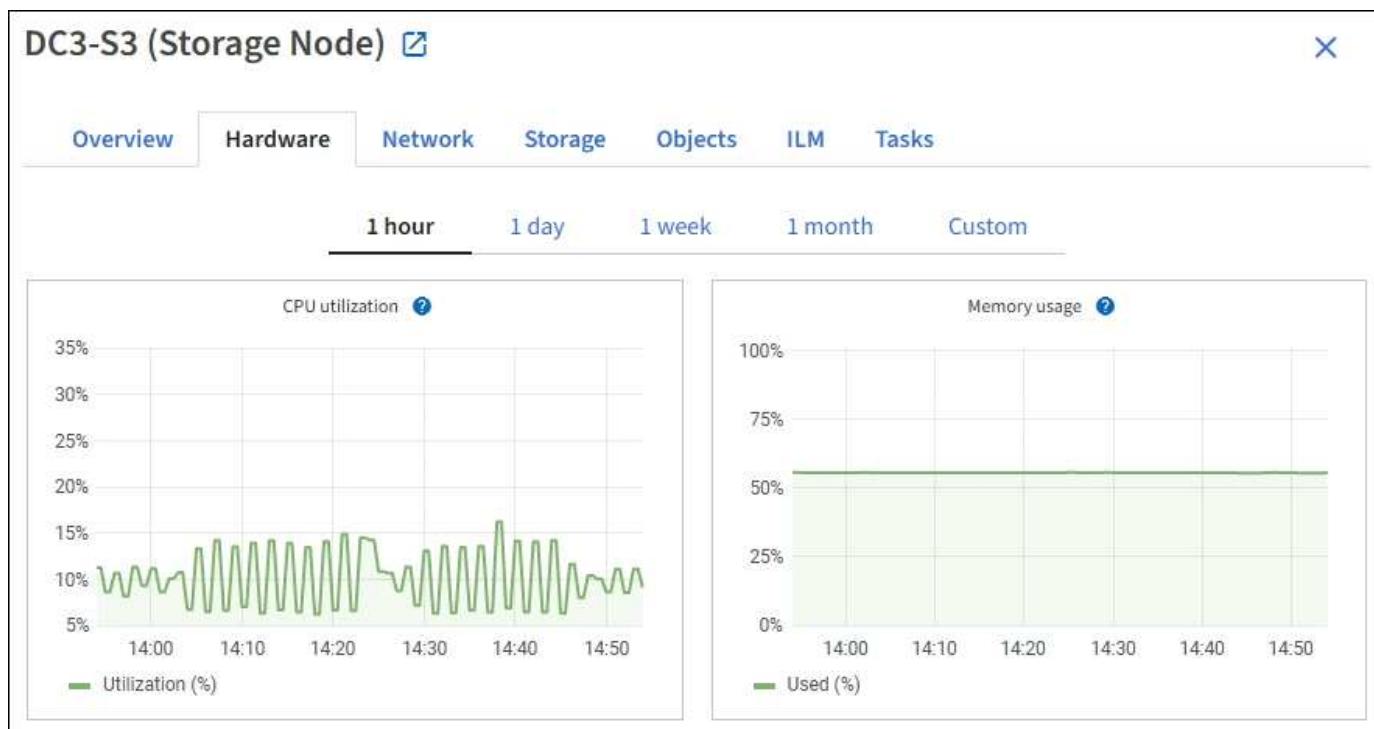
Vea la pestaña hardware

En la pestaña hardware, se muestra la utilización de CPU y la memoria de cada nodo, así como información de hardware adicional sobre los dispositivos.



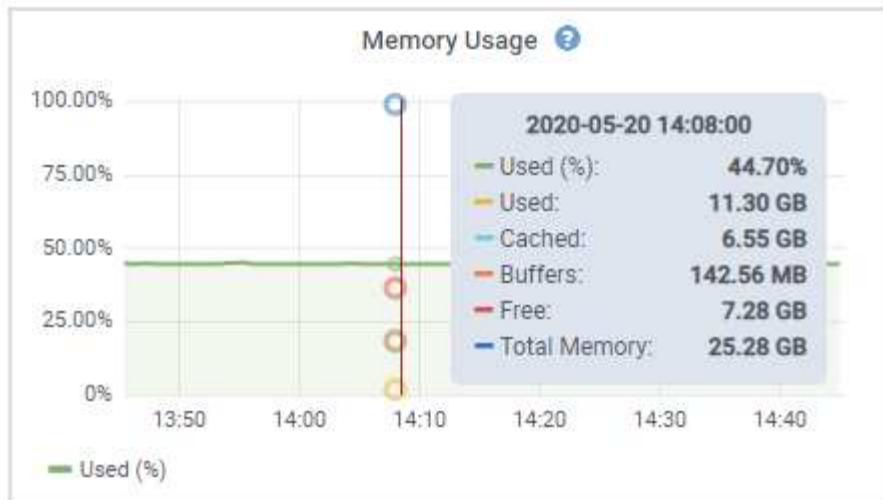
Grid Manager se actualiza con cada versión, por lo que es posible que no coincida con las capturas de pantalla de los ejemplos de esta página.

La pestaña hardware se muestra para todos los nodos.



Para mostrar un intervalo de tiempo diferente, seleccione uno de los controles situados encima del gráfico o gráfico. Puede visualizar la información disponible para intervalos de 1 hora, 1 día, 1 semana o 1 mes. También puede establecer un intervalo personalizado, que le permite especificar intervalos de fecha y hora.

Para ver detalles sobre el uso de la CPU y el uso de memoria, coloque el cursor sobre cada gráfico.



Si el nodo es un nodo de dispositivo, en esta pestaña también se incluye una sección con más información sobre el hardware del dispositivo.

Ver información sobre los nodos de almacenamiento de dispositivos

En la página Nodes, se incluye información sobre el estado del servicio y todos los recursos computacionales, de dispositivo de disco y de red para cada nodo de almacenamiento del dispositivo. También puede ver memoria, hardware de almacenamiento, versión del firmware de la controladora, recursos de red, interfaces de red, direcciones de red, y recibir y transmitir datos.

Pasos

1. En la página Nodes, seleccione un dispositivo Storage Node.
2. Seleccione **Descripción general**.

La sección Información de nodos de la ficha Descripción general muestra información de resumen del nodo, como el nombre, tipo, ID y estado de conexión del nodo. La lista de direcciones IP incluye el nombre de la interfaz de cada dirección de la siguiente manera:

- **Eth**: Red Grid, red de administración o red de cliente.
- **Clic**: Uno de los puertos 10, 25 o 100 GbE físicos del aparato. Estos puertos se pueden unir y conectar a la red de cuadrícula de StorageGRID (eth0) y a la red de cliente (eth2).
- * **mtc***: Uno de los puertos físicos de 1 GbE del aparato. Una o varias interfaces mtc se enlazan para formar la interfaz de red de administración de StorageGRID (eth1). Puede dejar disponibles otras interfaces mtc para la conectividad local temporal de un técnico en el centro de datos.

DC2-SGA-010-096-106-021 (Storage Node)



Overview **Hardware** Network Storage Objects ILM Tasks

Node information

| | |
|-------------------|--|
| Name: | DC2-SGA-010-096-106-021 |
| Type: | Storage Node |
| ID: | f0890e03-4c72-401f-ae92-245511a38e51 |
| Connection state: |  Connected |
| Storage used: | Object data  7%  Object metadata  5%  |
| Software version: | 11.6.0 (build 20210915.1941.afce2d9) |
| IP addresses: | 10.96.106.21 - eth0 (Grid Network) |

[Hide additional IP addresses](#) 

| Interface | IP address |
|---------------------|--------------------------|
| eth0 (Grid Network) | 10.96.106.21 |
| eth0 (Grid Network) | fe80::2a0:98ff:fe64:6582 |
| hic2 | 10.96.106.21 |
| hic4 | 10.96.106.21 |
| mtc2 | 169.254.0.1 |

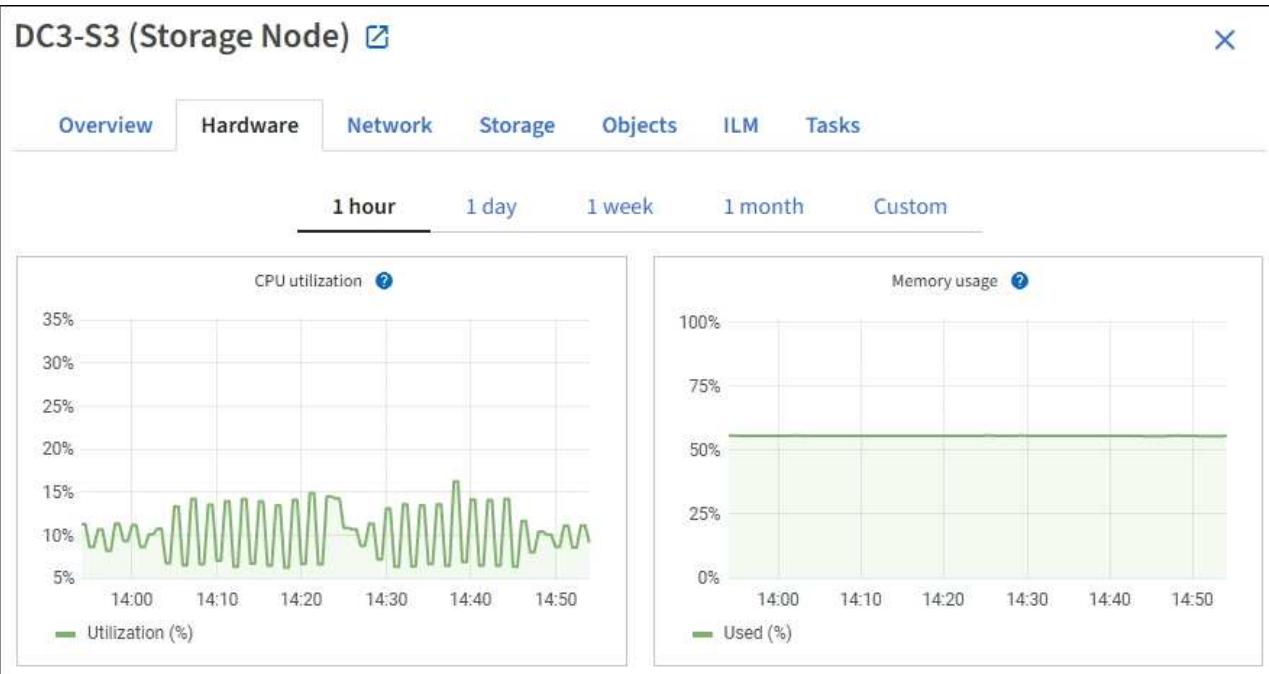
Alerts

| Alert name | Severity | Time triggered | Current values |
|--|---|---|--|
| ILM placement unachievable  |  Major | 2 hours ago  | A placement instruction in an ILM rule cannot be achieved for certain objects. |

En la sección Alerts de la pestaña Overview se muestran las alertas activas para el nodo.

3. Seleccione hardware para obtener más información sobre el dispositivo.

- Consulte los gráficos de utilización de CPU y memoria para determinar los porcentajes de uso de CPU y memoria a lo largo del tiempo. Para mostrar un intervalo de tiempo diferente, seleccione uno de los controles situados encima del gráfico o gráfico. Puede visualizar la información disponible para intervalos de 1 hora, 1 día, 1 semana o 1 mes. También puede establecer un intervalo personalizado, que le permite especificar intervalos de fecha y hora.



- b. Desplácese hacia abajo para ver la tabla de componentes del aparato. En esta tabla se incluye información como el nombre de modelo del dispositivo, los nombres de las controladoras, los números de serie y las direcciones IP, y el estado de cada componente.



Algunos campos, como el hardware de informática y IP de BMC Controller, aparecen solo para dispositivos con esa función.

Los componentes de las bandejas de almacenamiento y las bandejas de expansión si forman parte de la instalación se muestran en una tabla aparte debajo de la tabla del dispositivo.

StorageGRID Appliance

| | |
|---|---------------------------------|
| Appliance model: | SG6060 |
| Storage controller name: | StorageGRID-Lab79-SG6060-7-134 |
| Storage controller A management IP: | 10.2 [REDACTED] |
| Storage controller B management IP: | 10.2 [REDACTED] |
| Storage controller WWID: | 6d039ea0000173e5000000065b7b761 |
| Storage appliance chassis serial number: | 721924500068 |
| Storage controller firmware version: | 08.53.00.09 |
| Storage controller SANtricity OS version: | 11.50.3R2 |
| Storage controller NVSRAM version: | N280X-853834-DG1 |
| Storage hardware: | Nominal |
| Storage controller failed drive count: | 0 |
| Storage controller A: | Nominal |
| Storage controller B: | Nominal |
| Storage controller power supply A: | Nominal |
| Storage controller power supply B: | Nominal |
| Storage data drive type: | NL-SAS HDD |
| Storage data drive size: | 4.00 TB |
| Storage RAID mode: | DDP16 |
| Storage connectivity: | Nominal |
| Overall power supply: | Degraded |
| Compute controller BMC IP: | 10.2 [REDACTED] |
| Compute controller serial number: | 721917500060 |
| Compute hardware: | Needs Attention |
| Compute controller CPU temperature: | Nominal |
| Compute controller chassis temperature: | Nominal |
| Compute controller power supply A: | Failed |
| Compute controller power supply B: | Nominal |

Storage shelves

| Shelf chassis serial number | Shelf ID | Shelf status | IDOM status | Power supply status | Drawer status | Fan status |
|-----------------------------|----------|--------------|-------------|---------------------|---------------|------------|
| 721924500068 | 99 | Nominal | N/A | Nominal | Nominal | Nominal |

| En la tabla dispositivo | Descripción |
|---|--|
| Modelo de dispositivo | El número de modelo de este dispositivo StorageGRID se muestra en SANtricity OS. |
| Nombre de la controladora de almacenamiento | El nombre de este dispositivo StorageGRID se muestra en el sistema operativo SANtricity. |
| IP de administración de la controladora de almacenamiento a | La dirección IP del puerto de gestión 1 en la controladora de almacenamiento A. Utilice esta IP para acceder a SANtricity OS para solucionar problemas de almacenamiento. |
| IP de gestión de la controladora de almacenamiento B. | La dirección IP del puerto de gestión 1 en la controladora de almacenamiento B. Utilice esta IP para acceder a SANtricity OS para solucionar los problemas de almacenamiento. Algunos modelos de dispositivos no tienen una controladora de almacenamiento B. |

| En la tabla dispositivo | Descripción |
|---|---|
| WWID de la controladora de almacenamiento | El identificador a nivel mundial de la controladora de almacenamiento que se muestra en el sistema operativo SANtricity. |
| Número de serie del chasis del dispositivo de almacenamiento | El número de serie del chasis del dispositivo. |
| La versión de firmware de la controladora de almacenamiento | La versión del firmware en el controlador de almacenamiento para este dispositivo. |
| Versión del sistema operativo SANtricity de la controladora de almacenamiento | La versión de sistema operativo SANtricity de la controladora de almacenamiento A. |
| Versión de NVSRAM de la controladora de almacenamiento | <p>La versión de NVSRAM de la controladora de almacenamiento, según lo informado por SANtricity System Manager.</p> <p>Para SG6060 y SG6160, si hay una discrepancia de versión de NVSRAM entre las dos controladoras, muestra la versión de la controladora A. Si la controladora A no está instalada ni operativa, muestra la versión de la controladora B.</p> |
| Hardware de almacenamiento | <p>El estado general del hardware de la controladora de almacenamiento. Si System Manager de SANtricity informa sobre el estado de necesita atención para el hardware de almacenamiento, el sistema StorageGRID también informa de este valor.</p> <p>Si el estado es «Necesita atención», compruebe primero la controladora de almacenamiento con SANtricity OS. A continuación, asegúrese de que no exista ninguna otra alerta que se aplique a la controladora de computación.</p> |
| El número de unidades que la controladora de almacenamiento no pudo completar | La cantidad de unidades que no se encuentran en estado óptimo. |
| Controladora de almacenamiento A | El estado de la controladora de almacenamiento A. |
| Controladora de almacenamiento B | El estado de la controladora de almacenamiento B. Algunos modelos de dispositivos no tienen una controladora de almacenamiento B. |
| La controladora de almacenamiento proporciona alimentación A | El estado de suministro de alimentación A para la controladora de almacenamiento. |
| Suministro de alimentación de la controladora de almacenamiento B | El estado del suministro de alimentación B para la controladora de almacenamiento. |

| En la tabla dispositivo | Descripción |
|--|---|
| Tipo de unidad de datos de almacenamiento | El tipo de unidades en el dispositivo, como HDD (unidad de disco duro) o SSD (unidad de estado sólido). |
| Tamaño de las unidades de datos de almacenamiento | <p>El tamaño efectivo de una unidad de datos.</p> <p>Para SG6160, también se muestra el tamaño de la unidad de caché.</p> <p>Nota: Para los nodos con estantes de expansión, utilice el El tamaño de las unidades de datos de cada bandeja en su lugar. El tamaño de unidad efectivo puede diferir en función de la bandeja.</p> |
| Modo RAID de almacenamiento | El modo RAID configurado para el dispositivo. |
| Conectividad del almacenamiento | Estado de la conectividad del almacenamiento. |
| Suministro de alimentación general | El estado de todas las fuentes de alimentación del dispositivo. |
| BMC IP de la controladora de computación | <p>La dirección IP del puerto del controlador de administración de la placa base (BMC) en el controlador de computación. Utilice esta IP para conectarse a la interfaz del BMC para supervisar y diagnosticar el hardware del dispositivo.</p> <p>Este campo no se muestra para los modelos de dispositivos que no contienen una BMC.</p> |
| Número de serie de la controladora de computación | El número de serie de la controladora de computación. |
| Hardware de computación | El estado del hardware de la controladora de computación. Este campo no se muestra para los modelos de dispositivos que no tienen hardware de computación y hardware de almacenamiento independientes. |
| Temperatura de CPU de la controladora de computación | El estado de temperatura de la CPU de la controladora de computación. |
| Temperatura del chasis de la controladora de computación | El estado de temperatura de la controladora de computación. |

+

| En la tabla bandejas de almacenamiento | Descripción |
|---|--|
| Número de serie del chasis de la bandeja | El número de serie del chasis de la bandeja de almacenamiento. |

| En la tabla bandejas de almacenamiento | Descripción |
|--|--|
| ID de bandeja | <p>El identificador numérico de la bandeja de almacenamiento.</p> <ul style="list-style-type: none"> • 99: Bandeja de controladoras de almacenamiento • 0: Primer estante de expansión • 1: Segunda bandeja de expansión <p>Nota: Los estantes de expansión solo se aplican a los modelos SG6060 y SG6160.</p> |
| Estado de bandeja | El estado general de la bandeja de almacenamiento. |
| Estado de IOM | El estado de los módulos de entrada/salida (IOM) en cualquier bandeja de expansión. N/A si no se trata de una bandeja de ampliación. |
| Estado de suministros de alimentación | El estado general de los suministros de alimentación para la bandeja de almacenamiento. |
| Estado de cajón | El estado de los cajones en la bandeja de almacenamiento. N/A si la bandeja no contiene cajones. |
| Estado de ventiladores | El estado general de los ventiladores de refrigeración de la bandeja de almacenamiento. |
| Ranuras de unidades | El número total de ranuras de unidades de la bandeja de almacenamiento. |
| Unidades de datos | La cantidad de unidades de la bandeja de almacenamiento que se usan para el almacenamiento de datos. |
| Tamaño de la unidad de datos | El tamaño efectivo de una unidad de datos en la bandeja de almacenamiento. |
| Unidades en caché | La cantidad de unidades de la bandeja de almacenamiento que se usan como caché. |
| Tamaño de la unidad de caché | El tamaño de la unidad de caché más pequeña de la bandeja de almacenamiento. Normalmente, las unidades de caché tienen el mismo tamaño. |
| Estado de configuración | El estado de configuración de la bandeja de almacenamiento. |

a. Confirmar que todos los estados son nominales.

Si un estado no es nominal, revise las alertas actuales. También puede usar System Manager de

SANtricity para obtener más información acerca de estos valores de hardware. Consulte las instrucciones de instalación y mantenimiento del aparato.

4. Seleccione **Red** para ver la información de cada red.

El gráfico tráfico de red proporciona un resumen del tráfico de red general.



a. Revise la sección Network interfaces.

| Network interfaces | | | | | |
|--------------------|-------------------|------------|--------|------------------|-------------|
| Name | Hardware address | Speed | Duplex | Auto-negotiation | Link status |
| eth0 | 00:50:56:A7:66:75 | 10 Gigabit | Full | Off | Up |

Utilice la siguiente tabla con los valores de la columna **velocidad** de la tabla interfaces de red para determinar si los puertos de red 10/25-GbE del dispositivo se han configurado para utilizar el modo activo/backup o el modo LACP.



Los valores mostrados en la tabla asumen que se utilizan los cuatro enlaces.

| Modo de enlace | Modo de agregación | Velocidad de enlace de HIC individual (hipo 1, hipo 2, hipo 4) | Velocidad esperada de la red Grid/cliente (eth0,eth2) |
|----------------|--------------------|--|---|
| Agregado | LACP | 25 | 100 |
| Fija | LACP | 25 | 50 |
| Fija | Activa/Backup | 25 | 25 |
| Agregado | LACP | 10 | 40 |
| Fija | LACP | 10 | 20 |

| Modo de enlace | Modo de agregación | Velocidad de enlace de HIC individual (hipo 1, hipo 2, hipo 4) | Velocidad esperada de la red Grid/cliente (eth0,eth2) |
|----------------|--------------------|--|---|
| Fija | Activa/Backup | 10 | 10 |

Consulte "[Configure los enlaces de red](#)" para obtener más información sobre la configuración de los puertos 10/25-GbE.

b. Revise la sección Comunicación de red.

Las tablas de recepción y transmisión muestran cuántos bytes y paquetes se han recibido y enviado a través de cada red, así como otras métricas de recepción y transmisión.

Network communication

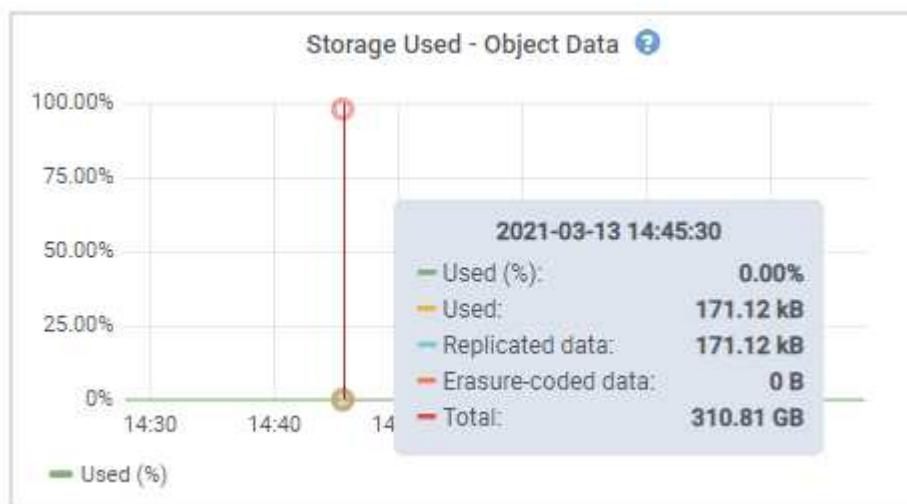
Receive

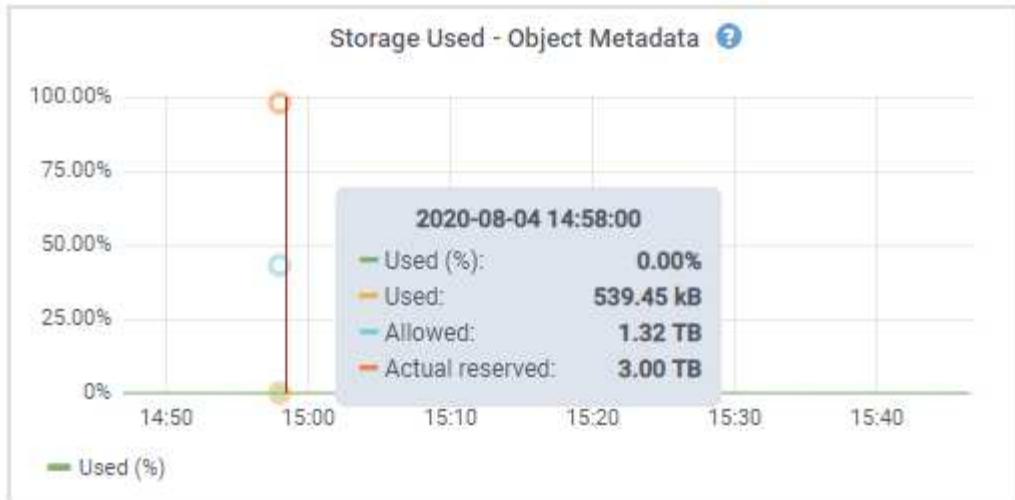
| Interface | Data | Packets | Errors | Dropped | Frame overruns | Frames |
|-----------|---------|------------|--------|---------|----------------|--------|
| eth0 | 2.89 GB | 19,421,503 | 0 | 24,032 | 0 | 0 |

Transmit

| Interface | Data | Packets | Errors | Dropped | Collisions | Carrier |
|-----------|---------|------------|--------|---------|------------|---------|
| eth0 | 3.64 GB | 18,494,381 | 0 | 0 | 0 | 0 |

5. Seleccione **almacenamiento** para ver gráficos que muestran los porcentajes de almacenamiento utilizados a lo largo del tiempo para los metadatos de objetos y datos de objetos, así como información sobre dispositivos de disco, volúmenes y almacenes de objetos.





- Desplácese hacia abajo para ver la cantidad de almacenamiento disponible para cada volumen y almacén de objetos.

El nombre a nivel mundial de cada disco coincide con el identificador a nivel mundial (WWID) del volumen que aparece cuando se visualizan las propiedades del volumen estándar en SANtricity OS (el software de gestión conectado a la controladora de almacenamiento del dispositivo).

Para ayudarle a interpretar las estadísticas de lectura y escritura del disco relacionadas con los puntos de montaje del volumen, la primera parte del nombre que aparece en la columna **Nombre** de la tabla dispositivos de disco (es decir, *sdc*, *sdd*, *sde*, etc.) coincide con el valor que se muestra en la columna **dispositivo** de la tabla de volúmenes.

| Disk devices | | | | | |
|-----------------|-----------------|----------|-----------|------------|--|
| Name | World Wide Name | I/O load | Read rate | Write rate | |
| croot(8:1,sda1) | N/A | 0.04% | 0 bytes/s | 3 KB/s | |
| cvloc(8:2,sda2) | N/A | 0.67% | 0 bytes/s | 50 KB/s | |
| sdc(8:16,sdb) | N/A | 0.03% | 0 bytes/s | 4 KB/s | |
| sdd(8:32,sdc) | N/A | 0.00% | 0 bytes/s | 82 bytes/s | |
| sde(8:48,sdd) | N/A | 0.00% | 0 bytes/s | 82 bytes/s | |

| Volumes | | | | | |
|----------------------|--------|--------|-----------|-----------|--------------------|
| Mount point | Device | Status | Size | Available | Write cache status |
| / | croot | Online | 21.00 GB | 14.75 GB | Unknown |
| /var/local | cvloc | Online | 85.86 GB | 84.05 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 |

| Object stores | | | | | | |
|---------------|-----------|-----------|-----------------|---------|-----------------|-----------|
| ID | Size | Available | Replicated data | EC data | Object data (%) | Health |
| 0000 | 107.32 GB | 96.44 GB | 124.60 KB | 0 bytes | 0.00% | No Errors |
| 0001 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0002 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |

Consulte información sobre los nodos de administración del dispositivo y los nodos de puerta de enlace

En la página Nodes, se incluye información sobre el estado del servicio y todos los recursos computacionales, de disco y de red para cada dispositivo de servicios que se utiliza como nodo de administración o nodo de puerta de enlace. También puede ver memoria, hardware de almacenamiento, recursos de red, interfaces de red, direcciones de red, y recibir y transmitir datos.

Pasos

1. En la página Nodes, seleccione un nodo de administrador de dispositivos o un Appliance Gateway Node.
2. Seleccione **Descripción general**.

La sección Información de nodos de la ficha Descripción general muestra información de resumen del nodo, como el nombre, tipo, ID y estado de conexión del nodo. La lista de direcciones IP incluye el nombre

de la interfaz de cada dirección de la siguiente manera:

- **Adllb** y **adlli**: Se muestra si se utiliza el enlace activo/de respaldo para la interfaz de red de administración
- **Eth**: Red Grid, red de administración o red de cliente.
- **Clic**: Uno de los puertos 10, 25 o 100 GbE físicos del aparato. Estos puertos se pueden unir y conectar a la red de cuadrícula de StorageGRID (eth0) y a la red de cliente (eth2).
- * **mtc***: Uno de los puertos 1-GbE físicos del aparato. Una o más interfaces mtc se vinculan para formar la interfaz de red de administración (eth1). Puede dejar disponibles otras interfaces mtc para la conectividad local temporal de un técnico en el centro de datos.

The screenshot shows the SANtricity System Manager interface for the node 10-224-6-199-ADM1. The top navigation bar includes tabs for Overview, Hardware, Network, Storage, Load balancer, Tasks, and SANtricity System Manager. The Network tab is selected. Below the tabs, the 'Node information' section displays the following details:

| | |
|-------------------|--|
| Name: | 10-224-6-199-ADM1 |
| Type: | Primary Admin Node |
| ID: | 6fdc1890-ca0a-4493-acdd-72ed317d95fb |
| Connection state: | Connected |
| Software version: | 11.6.0 (build 20210928.1321.6687ee3) |
| IP addresses: | 172.16.6.199 - eth0 (Grid Network) 10.224.6.199 - eth1 (Admin Network) 47.47.7.241 - eth2 (Client Network) |

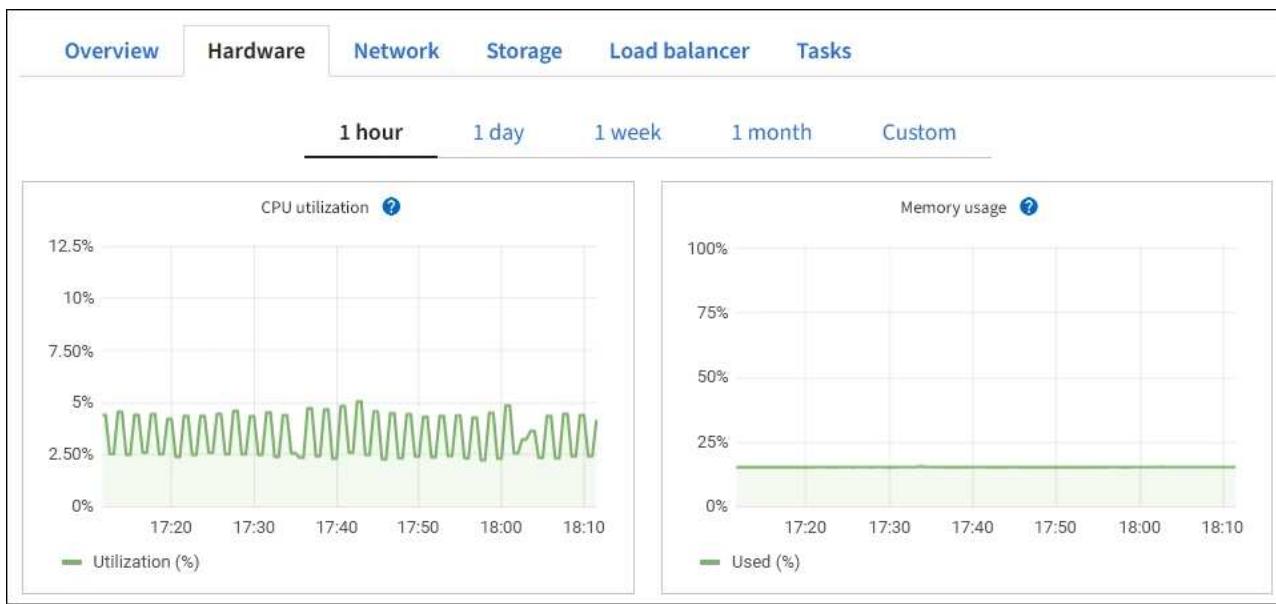
Below this, there is a link to 'Hide additional IP addresses'. A scrollable table lists the network interfaces and their corresponding IP addresses:

| Interface | IP address |
|-----------------------|-----------------------------------|
| eth2 (Client Network) | 47.47.7.241 |
| eth2 (Client Network) | fd20:332:332:0:e42:a1ff:fe86:b5b0 |
| eth2 (Client Network) | fe80::e42:a1ff:fe86:b5b0 |
| hic1 | 47.47.7.241 |
| hic2 | 47.47.7.241 |
| hic3 | 47.47.7.241 |

En la sección Alerts de la pestaña Overview se muestran las alertas activas para el nodo.

3. Seleccione **hardware** para obtener más información sobre el dispositivo.

- Consulte los gráficos de utilización de CPU y memoria para determinar los porcentajes de uso de CPU y memoria a lo largo del tiempo. Para mostrar un intervalo de tiempo diferente, seleccione uno de los controles situados encima del gráfico o gráfico. Puede visualizar la información disponible para intervalos de 1 hora, 1 día, 1 semana o 1 mes. También puede establecer un intervalo personalizado, que le permite especificar intervalos de fecha y hora.



- b. Desplácese hacia abajo para ver la tabla de componentes del aparato. Esta tabla contiene información, como el nombre del modelo, número de serie, versión de firmware de la controladora y el estado de cada componente.

| StorageGRID Appliance | | |
|---|-----------------|---|
| Appliance model: | SG100 | ? |
| Storage controller failed drive count: | 0 | ! |
| Storage data drive type: | SSD | ! |
| Storage data drive size: | 960.20 GB | ! |
| Storage RAID mode: | RAID1 [healthy] | ! |
| Storage connectivity: | Nominal | ! |
| Overall power supply: | Nominal | ! |
| Compute controller BMC IP: | 10.60.8.38 | ! |
| Compute controller serial number: | 372038000093 | ! |
| Compute hardware: | Nominal | ! |
| Compute controller CPU temperature: | Nominal | ! |
| Compute controller chassis temperature: | Nominal | ! |
| Compute controller power supply A: | Nominal | ! |
| Compute controller power supply B: | Nominal | ! |

| En la tabla dispositivo | Descripción |
|-------------------------|--|
| Modelo de dispositivo | El número de modelo para este dispositivo StorageGRID. |

| En la tabla dispositivo | Descripción |
|---|--|
| El número de unidades que la controladora de almacenamiento no pudo completar | La cantidad de unidades que no se encuentran en estado óptimo. |
| Tipo de unidad de datos de almacenamiento | El tipo de unidades en el dispositivo, como HDD (unidad de disco duro) o SSD (unidad de estado sólido). |
| Tamaño de las unidades de datos de almacenamiento | El tamaño efectivo de una unidad de datos. |
| Modo RAID de almacenamiento | El modo RAID del dispositivo. |
| Suministro de alimentación general | El estado de todas las fuentes de alimentación del dispositivo. |
| BMC IP de la controladora de computación | <p>La dirección IP del puerto del controlador de administración de la placa base (BMC) en el controlador de computación. Puede utilizar esta IP para conectarse a la interfaz del BMC para supervisar y diagnosticar el hardware del dispositivo.</p> <p>Este campo no se muestra para los modelos de dispositivos que no contienen una BMC.</p> |
| Número de serie de la controladora de computación | El número de serie de la controladora de computación. |
| Hardware de computación | El estado del hardware de la controladora de computación. |
| Temperatura de CPU de la controladora de computación | El estado de temperatura de la CPU de la controladora de computación. |
| Temperatura del chasis de la controladora de computación | El estado de temperatura de la controladora de computación. |

a. Confirmar que todos los estados son nominales.

Si un estado no es nominal, revise las alertas actuales.

4. Seleccione **Red** para ver la información de cada red.

El gráfico tráfico de red proporciona un resumen del tráfico de red general.



a. Revise la sección Network interfaces.

| Network interfaces | | | | | |
|--------------------|-------------------|-------------|--------|------------------|-------------|
| Name | Hardware address | Speed | Duplex | Auto-negotiation | Link status |
| eth0 | 0C:42:A1:86:B5:B0 | 100 Gigabit | Full | Off | Up |
| eth1 | B4:A9:FC:71:68:36 | Gigabit | Full | Off | Up |
| eth2 | 0C:42:A1:86:B5:B0 | 100 Gigabit | Full | Off | Up |
| hic1 | 0C:42:A1:86:B5:B0 | 25 Gigabit | Full | On | Up |
| hic2 | 0C:42:A1:86:B5:B0 | 25 Gigabit | Full | On | Up |
| hic3 | 0C:42:A1:86:B5:B0 | 25 Gigabit | Full | On | Up |
| hic4 | 0C:42:A1:86:B5:B0 | 25 Gigabit | Full | On | Up |
| mtc1 | B4:A9:FC:71:68:36 | Gigabit | Full | On | Up |
| mtc2 | B4:A9:FC:71:68:35 | Gigabit | Full | On | Up |

Utilice la siguiente tabla con los valores de la columna **velocidad** de la tabla interfaces de red para determinar si los cuatro puertos de red 40/100-GbE del dispositivo estaban configurados para utilizar el modo activo/backup o el modo LACP.



Los valores mostrados en la tabla asumen que se utilizan los cuatro enlaces.

| Modo de enlace | Modo de agregación | Velocidad de enlace de HIC individual (hipo 1, hipo 2, hipo 4) | Velocidad esperada de la red Grid/cliente (eth0, eth2) |
|----------------|--------------------|--|--|
| Agregado | LACP | 100 | 400 |
| Fija | LACP | 100 | 200 |
| Fija | Activa/Backup | 100 | 100 |
| Agregado | LACP | 40 | 160 |
| Fija | LACP | 40 | 80 |
| Fija | Activa/Backup | 40 | 40 |

b. Revise la sección Comunicación de red.

Las tablas de recepción y transmisión muestran cuántos bytes y paquetes se han recibido y enviado a través de cada red, así como otras métricas de recepción y transmisión.

| Network communication | | | | | | | |
|-----------------------|---------|------------|--------|---------|----------------|---------|--|
| Receive | | | | | | | |
| Interface | Data | Packets | Errors | Dropped | Frame overruns | Frames | |
| eth0 | 2.89 GB | 19,421,503 | 0 | 24,032 | 0 | 0 | |
| Transmit | | | | | | | |
| Interface | Data | Packets | Errors | Dropped | Collisions | Carrier | |
| eth0 | 3.64 GB | 18,494,381 | 0 | 0 | 0 | 0 | |

5. Seleccione **almacenamiento** para ver información sobre los dispositivos de disco y los volúmenes del dispositivo de servicios.

DO-REF-DC1-GW1 (Gateway Node)



Overview Hardware Network Storage Load balancer Tasks

Disk devices

| Name | World Wide Name | I/O load | Read rate | Write rate |
|-----------------|-----------------|----------|-----------|------------|
| croot(8:1,sda1) | N/A | 0.02% | 0 bytes/s | 3 KB/s |
| cvloc(8:2,sda2) | N/A | 0.03% | 0 bytes/s | 6 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 | 84.63 GB  | Unknown |

Abra la pestaña Network

La pestaña Red muestra un gráfico que muestra el tráfico de red recibido y enviado a través de todas las interfaces de red del nodo, sitio o cuadrícula.

La pestaña Red se muestra para todos los nodos, sitios y toda la cuadrícula.

Para mostrar un intervalo de tiempo diferente, seleccione uno de los controles situados encima del gráfico o gráfico. Puede visualizar la información disponible para intervalos de 1 hora, 1 día, 1 semana o 1 mes. También puede establecer un intervalo personalizado, que le permite especificar intervalos de fecha y hora.

Para los nodos, la tabla de interfaces de red proporciona información acerca de los puertos de red física de cada nodo. La tabla de comunicaciones de red proporciona detalles acerca de las operaciones de recepción y transmisión de cada nodo y de cualquier contador de fallos informado por el controlador.

DC1-S2 (Storage Node)

Overview Hardware **Network** Storage Objects ILM Tasks

1 hour 1 day 1 week 1 month Custom

Network traffic

650 kb/s
600 kb/s
550 kb/s
500 kb/s
450 kb/s

Received Sent

10:05 10:10 10:15 10:20 10:25 10:30 10:35 10:40 10:45 10:50 10:55 11:00

Network interfaces

| Name | Hardware address | Speed | Duplex | Auto-negotiation | Link status |
|------|-------------------|------------|--------|------------------|-------------|
| eth0 | 00:50:56:A7:E8:1D | 10 Gigabit | Full | Off | Up |

Network communication

Receive

| Interface | Data | Packets | Errors | Dropped | Frame overruns | Frames |
|-----------|---------|------------|--------|---------|----------------|--------|
| eth0 | 3.04 GB | 20,403,428 | 0 | 24,899 | 0 | 0 |

Transmit

| Interface | Data | Packets | Errors | Dropped | Collisions | Carrier |
|-----------|---------|------------|--------|---------|------------|---------|
| eth0 | 3.65 GB | 19,061,947 | 0 | 0 | 0 | 0 |

Información relacionada

["Supervisar las conexiones de red y el rendimiento"](#)

Consulte la pestaña almacenamiento

La pestaña almacenamiento resume la disponibilidad del almacenamiento y otras medidas relacionadas con él.

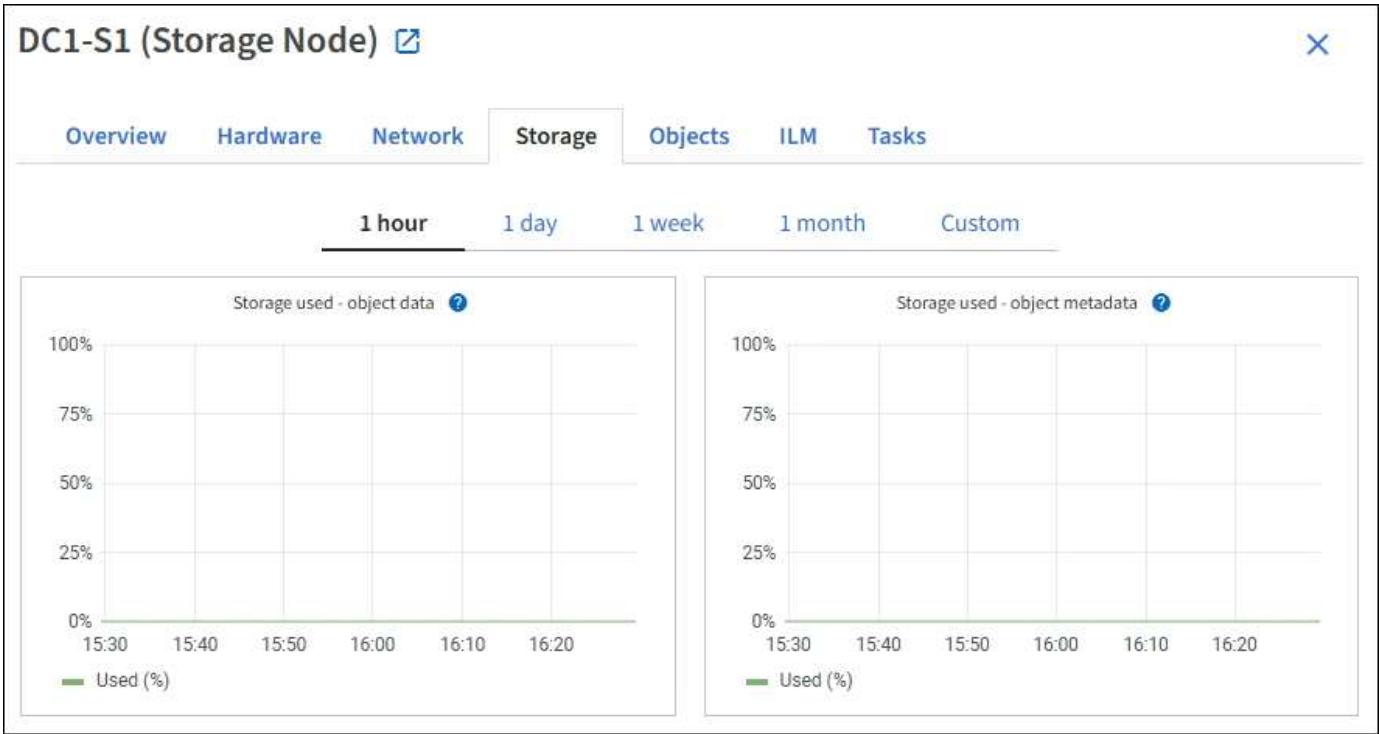
La pestaña almacenamiento se muestra para todos los nodos, cada sitio y toda la cuadrícula.

Gráficos de uso del almacenamiento

En los nodos de almacenamiento, cada sitio y toda la cuadrícula, la pestaña almacenamiento incluye gráficos que muestran cuánto almacenamiento han utilizado los datos de objetos y los metadatos de objetos a lo largo del tiempo.



Cuando un nodo no está conectado a la cuadrícula, como durante la actualización o un estado desconectado, es posible que algunas métricas no estén disponibles o se excluyan de los totales de la ubicación y la cuadrícula. Después de que un nodo se vuelva a conectar a la cuadrícula, espere varios minutos para que los valores se estabilicen.



Dispositivos de disco, volúmenes y almacenes de objetos

Para todos los nodos, la ficha almacenamiento contiene detalles de los dispositivos de disco y volúmenes del nodo. Para los nodos de almacenamiento, la tabla Object Stores proporciona información sobre cada volumen de almacenamiento.

| Disk devices | | | | | |
|-----------------|-----------------|----------|-----------|------------|--|
| Name | World Wide Name | I/O load | Read rate | Write rate | |
| croot(8:1,sda1) | N/A | 0.04% | 0 bytes/s | 3 KB/s | |
| cvloc(8:2,sda2) | N/A | 0.67% | 0 bytes/s | 50 KB/s | |
| sdc(8:16,sdb) | N/A | 0.03% | 0 bytes/s | 4 KB/s | |
| sdd(8:32,sdc) | N/A | 0.00% | 0 bytes/s | 82 bytes/s | |
| sde(8:48,sdd) | N/A | 0.00% | 0 bytes/s | 82 bytes/s | |

| Volumes | | | | | |
|----------------------|--------|--------|-----------|-----------|--------------------|
| Mount point | Device | Status | Size | Available | Write cache status |
| / | croot | Online | 21.00 GB | 14.75 GB | Unknown |
| /var/local | cvloc | Online | 85.86 GB | 84.05 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 |

| Object stores | | | | | | | |
|---------------|-----------|-----------|-----------------|---------|-----------------|-----------|--|
| ID | Size | Available | Replicated data | EC data | Object data (%) | Health | |
| 0000 | 107.32 GB | 96.44 GB | 124.60 KB | 0 bytes | 0.00% | No Errors | |
| 0001 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors | |
| 0002 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors | |

Información relacionada

"Supervise la capacidad de almacenamiento"

Abra la pestaña objetos

El separador Objetos proporciona información sobre "S3 tasas de procesamiento y recuperación".

La pestaña Objects se muestra para cada nodo de almacenamiento, cada sitio y toda la cuadrícula. Para los nodos de almacenamiento, la pestaña Objects también proporciona información y recuentos de objetos acerca de consultas de metadatos y verificación en segundo plano.

Vea la pestaña ILM

La pestaña ILM proporciona información sobre las operaciones de gestión de la vida útil de la información (ILM).

La pestaña ILM se muestra para cada nodo de almacenamiento, cada sitio y toda la cuadrícula. Para cada sitio y la cuadrícula, la pestaña ILM muestra un gráfico de la cola de ILM a lo largo del tiempo. Para el grid, esta pestaña también proporciona el tiempo estimado para completar un análisis de ILM completo de todos los objetos.

En el caso de los nodos de almacenamiento, la pestaña ILM proporciona detalles sobre la evaluación de ILM y la verificación en segundo plano para los objetos con código de borrado.

DC2-S1 (Storage Node)

Overview Hardware Network Storage Objects **ILM** Tasks

Evaluation

| | | |
|--------------------|---|---|
| Awaiting - all: |  0 objects |  |
| Awaiting - client: |  0 objects |  |
| Evaluation rate: |  0.00 objects / second | |
| Scan rate: |  0.00 objects / second |  |

Erasure coding verification

| | | |
|---------------------|---|---|
| Status: |  Idle |  |
| Next scheduled: |  2021-09-09 17:36:44 MDT | |
| Fragments verified: |  0 |  |
| Data verified: |  0 bytes |  |
| Corrupt copies: |  0 |  |
| Corrupt fragments: |  0 |  |
| Missing fragments: |  0 |  |

Información relacionada

- "Supervise la gestión del ciclo de vida de la información"
- "Administre StorageGRID"

Abra el separador Equilibrador de Carga

La pestaña Load Balancer incluye gráficos de rendimiento y diagnóstico relacionados con la operación del servicio Load Balancer.

La pestaña Load Balancer se muestra para los nodos de administrador y de puerta de enlace, cada sitio y todo el grid. Para cada sitio, la pestaña Load Balancer proporciona un resumen de las estadísticas de todos los nodos de ese sitio. Para toda la cuadrícula, la pestaña Load Balancer proporciona un resumen de las estadísticas de todos los sitios.

Si no se está ejecutando ninguna E/S a través del servicio de Equilibrador de Carga, o no hay ningún equilibrador de carga configurado, los gráficos muestran “No hay datos”.



Solicitar tráfico

Este gráfico proporciona una media móvil de 3 minutos del rendimiento de los datos transmitidos entre los extremos del equilibrador de carga y los clientes que realizan las solicitudes, en bits por segundo.



Este valor se actualiza al finalizar cada solicitud. Como resultado, este valor puede diferir del rendimiento en tiempo real a tasas de solicitud bajas o a solicitudes de larga duración. Puede consultar la ficha Red para obtener una vista más realista del comportamiento actual de la red.

Tasa de solicitudes entrantes

Este gráfico proporciona una media móvil de 3 minutos del número de nuevas solicitudes por segundo, desglosadas por tipo de solicitud (GET, PUT, HEAD y DELETE). Este valor se actualiza cuando se han validado los encabezados de una nueva solicitud.

Duración media de la solicitud (no error)

Este gráfico proporciona una media móvil de 3 minutos de duración de las solicitudes, desglosada por tipo de solicitud (GET, PUT, HEAD y DELETE). Cada duración de la solicitud comienza cuando el servicio Load Balancer analiza una cabecera de solicitud y finaliza cuando se devuelve el cuerpo de respuesta completo al cliente.

Tasa de respuesta de error

Este gráfico proporciona un promedio móvil de 3 minutos del número de respuestas de error devueltas a clientes por segundo, desglosado por el código de respuesta de error.

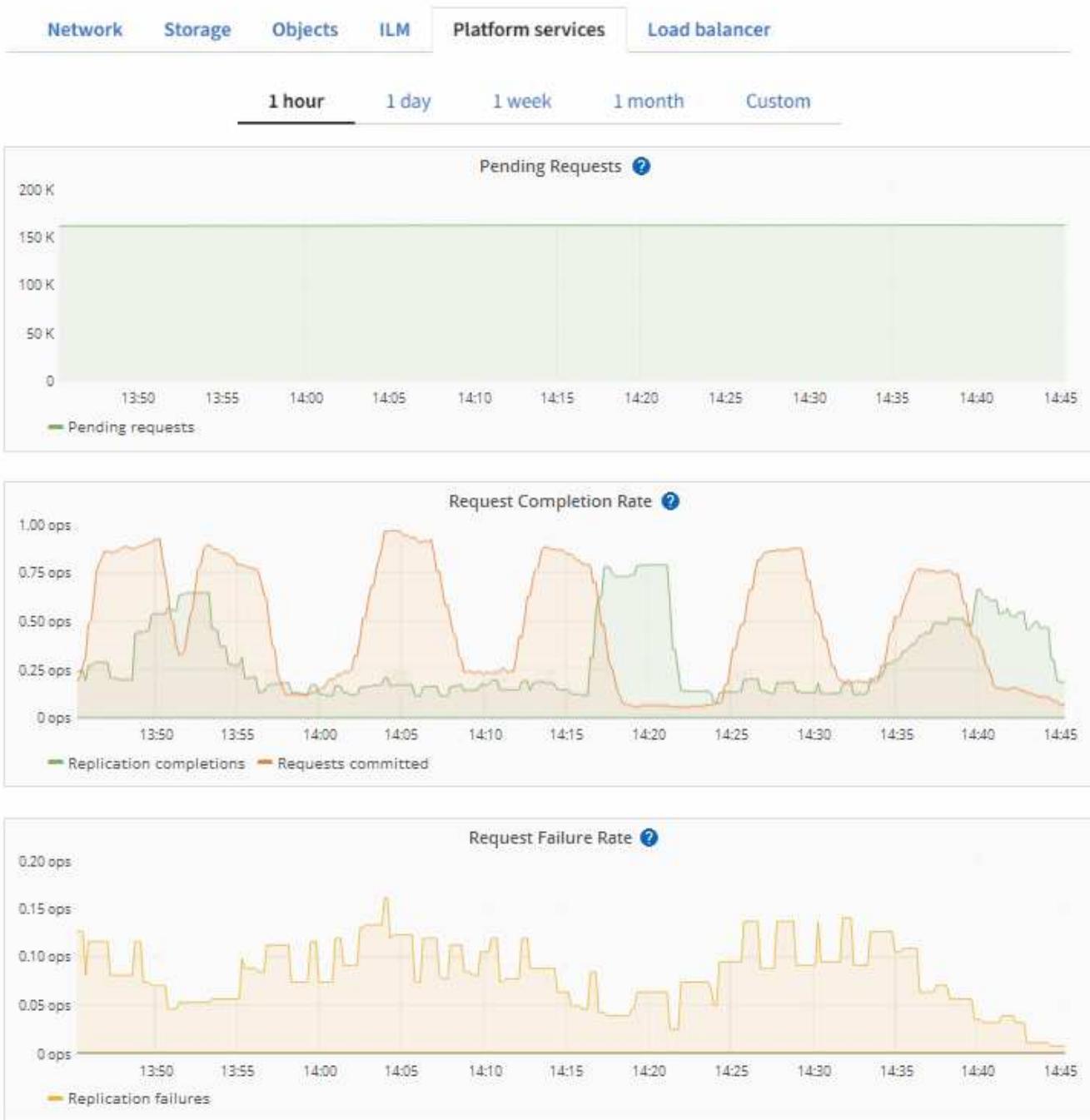
Información relacionada

- ["Supervisar las operaciones de equilibrio de carga"](#)
- ["Administre StorageGRID"](#)

Consulte la ficha Servicios de plataforma

La pestaña Servicios de plataforma proporciona información sobre cualquier operación de servicio de plataforma S3 en un sitio.

La ficha Servicios de plataforma se muestra para cada sitio. Esta pestaña proporciona información sobre servicios de plataforma S3, como la replicación de CloudMirror y el servicio de integración de búsqueda. Los gráficos de esta pestaña muestran métricas como el número de solicitudes pendientes, la tasa de finalización de solicitudes y la tasa de fallos de solicitud.



Para obtener más información sobre los servicios de la plataforma S3, incluidos los detalles de solución de problemas, consulte la "[Instrucciones para administrar StorageGRID](#)".

Consulte la pestaña Gestionar unidades

La pestaña Gestionar unidades permite acceder a los detalles y realizar tareas de solución de problemas y mantenimiento en las unidades de los dispositivos que admiten esta función.

En la pestaña Gestionar unidades, es posible hacer lo siguiente:

- Vea un diseño de las unidades de almacenamiento de datos en el dispositivo
- Vea una tabla que enumera cada ubicación, el tipo, el estado, la versión de firmware y el número de serie de la unidad
- Realice funciones de solución de problemas y mantenimiento en cada unidad

Para acceder a la pestaña Gestionar unidades, debe contar con la "[Permiso de acceso de administrador o de dispositivo de almacenamiento](#)".

Para obtener más información sobre el uso de la pestaña Gestionar unidades, consulte "[Use la pestaña Gestionar unidades](#)".

Ver la pestaña Administrador del sistema de SANtricity (solo E-Series)

La pestaña SANtricity System Manager le permite acceder a SANtricity System Manager sin necesidad de configurar ni conectar el puerto de gestión del dispositivo de almacenamiento. Puede utilizar esta pestaña para revisar la información de diagnóstico de hardware y entorno, así como los problemas relacionados con las unidades.

 Acceder a System Manager de SANtricity desde Grid Manager normalmente solo se utiliza para supervisar el hardware del dispositivo y configurar E-Series AutoSupport. Muchas funciones y operaciones de SANtricity System Manager, como la actualización del firmware, no se aplican a la supervisión de su dispositivo StorageGRID. Para evitar problemas, siga siempre las instrucciones de mantenimiento de hardware de su dispositivo. Para actualizar el firmware de SANtricity, consulte "[Procedimientos de configuración de mantenimiento](#)" el para el dispositivo de almacenamiento.

 La pestaña SANtricity System Manager solo se muestra para los nodos de dispositivos de almacenamiento donde se utiliza hardware de E-Series.

Con SANtricity System Manager, puede hacer lo siguiente:

- Vea datos de rendimiento como el rendimiento a nivel de cabina de almacenamiento, latencia de I/O, uso de CPU de la controladora de almacenamiento y rendimiento.
- Comprobar el estado de los componentes de hardware.
- Lleve a cabo funciones de soporte, como la visualización de datos de diagnóstico y la configuración de E-Series AutoSupport.

 Para utilizar System Manager de SANtricity y configurar un proxy para la AutoSupport de E-Series, consulte "[Envíe los paquetes AutoSupport de E-Series a través de StorageGRID](#)".

Para acceder a SANtricity System Manager mediante Grid Manager, es necesario contar con la "[Permiso de acceso de administrador o de dispositivo de almacenamiento](#)".

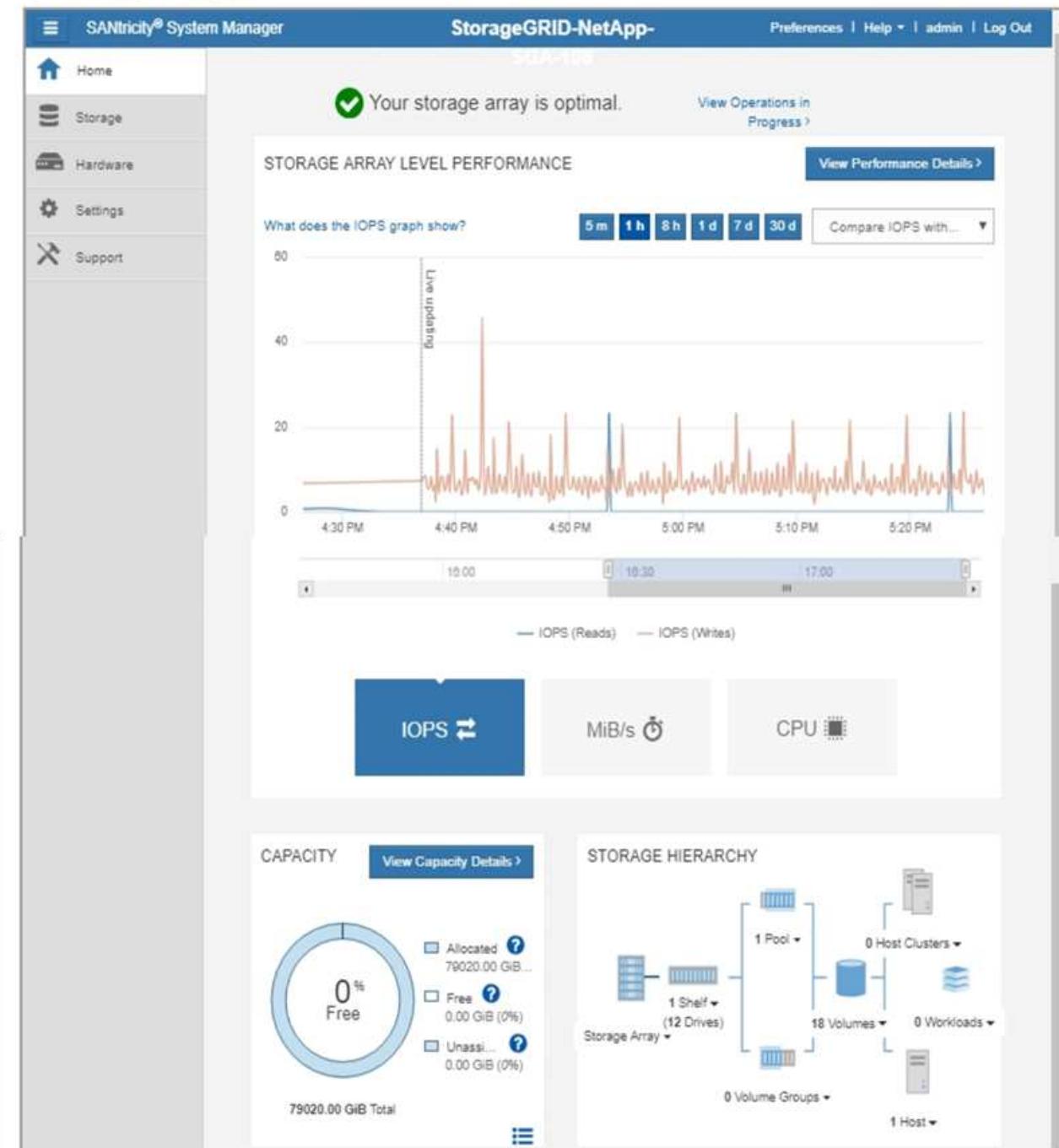
 Debe tener el firmware 8.70 de SANtricity o superior para acceder a SANtricity System Manager mediante Grid Manager.

La pestaña muestra la página de inicio de SANtricity System Manager.

Use SANtricity System Manager to monitor and manage the hardware components in this storage appliance. From SANtricity System Manager, you can review hardware diagnostic and environmental information as well as issues related to the drives.

Note: Many features and operations within SANtricity Storage Manager do not apply to your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance model.

Open SANtricity System Manager [\(S\)](#) in a new browser tab.



Puede usar el enlace SANtricity System Manager para abrir la instancia de SANtricity System Manager en una nueva ventana del navegador para facilitar la visualización.

Para ver detalles del rendimiento a nivel de la cabina de almacenamiento y el uso de capacidad, coloque el

cursor sobre cada gráfico.

Para obtener más detalles sobre la visualización de la información accesible desde la ficha Administrador del sistema de SANtricity, consulte "[Documentación de E-Series y SANtricity de NetApp](#)".

Información para monitorear regularmente

Qué y cuándo supervisar

Aunque el sistema de StorageGRID puede seguir funcionando cuando se producen errores o alguna parte del grid no está disponible, debe supervisar y solucionar posibles problemas antes de que afecten a la eficiencia o la disponibilidad del grid.

Antes de empezar

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

Acerca de las tareas de supervisión

Un sistema ocupado genera grandes cantidades de información. La siguiente lista proporciona orientación sobre la información más importante para supervisar de forma continua.

| Qué supervisar | Frecuencia |
|---|---|
| "Estado del sistema" | Diariamente |
| Ratio al que " Capacidad de metadatos y objetos de Storage Node " se está consumiendo | Semanal |
| "Operaciones de gestión del ciclo de vida de la información" | Semanal |
| "Redes y recursos del sistema" | Semanal |
| "Actividad de inquilino" | Semanal |
| "S3 operaciones cliente" | Semanal |
| "Operaciones de equilibrio de carga" | Tras la configuración inicial y tras cualquier cambio en la configuración |
| "Conexiones de federación de grid" | Semanal |

Supervise el estado del sistema

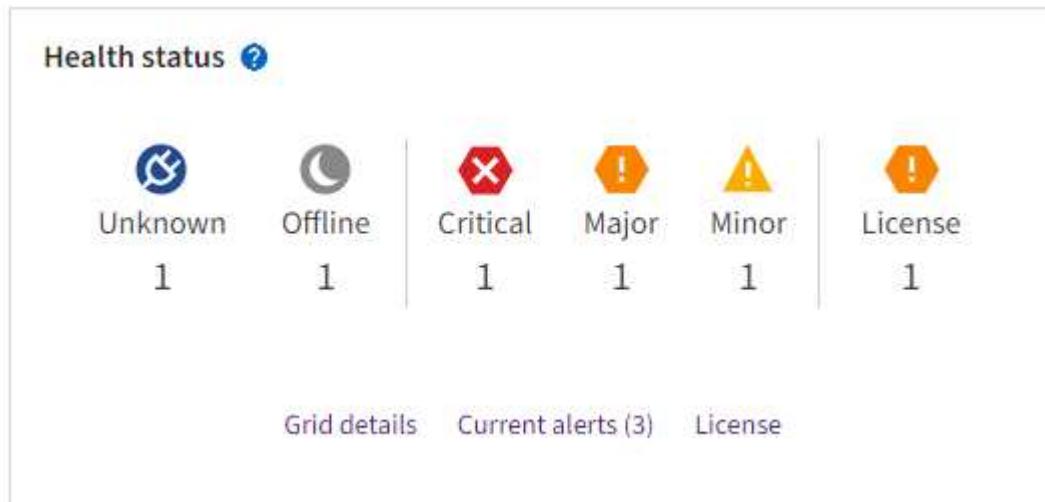
Supervise el estado general del sistema StorageGRID diariamente.

Acerca de esta tarea

El sistema StorageGRID puede seguir funcionando cuando algunas partes de la red no están disponibles. Los problemas potenciales que indican las alertas no son necesariamente problemas con las operaciones del

sistema. Investigue los problemas resumidos en la tarjeta de estado del panel de Grid Manager.

Para recibir notificaciones de alertas tan pronto como se activen, puede ["configurar notificaciones por correo electrónico para alertas"](#) o ["Configure las capturas SNMP"](#).



Cuando existen problemas, aparecen vínculos que le permiten ver detalles adicionales:

| Enlace | Aparece cuando... |
|---|---|
| Detalles de la cuadrícula | Todos los nodos están desconectados (estado de conexión desconocido o desconectado de forma administrativa). |
| Alertas actuales (críticas, principales, menores) | Las alertas son actualmente activo . |
| Alertas resueltas recientemente | Alertas activadas en la semana pasada ahora están resueltos . |
| Licencia | Hay un problema con la licencia de software de este sistema StorageGRID. Puede "actualice la información de licencia según sea necesario" . |

Supervise los estados de conexión de los nodos

Si uno o más nodos están desconectados de la cuadricula, es posible que se vean afectadas las operaciones críticas de StorageGRID. Supervise los estados de conexión de los nodos y resuelva cualquier problema con prontitud.

| | Descripción | Acción necesaria |
|--|--|---|
| | <p>No conectado - Desconocido</p> <p>Por una razón desconocida, un nodo está desconectado o los servicios del nodo se desactivan inesperadamente. Por ejemplo, un servicio del nodo podría estar detenido o podría haber perdido la conexión de red debido a un fallo de alimentación o a un corte inesperado.</p> <p>La alerta no se puede comunicar con el nodo también puede activarse. Otras alertas también pueden estar activas.</p> | <p>Requiere atención inmediata. Seleccione cada alerta y siga las acciones recomendadas.</p> <p>Por ejemplo, es posible que deba reiniciar un servicio que haya detenido o reiniciar el host del nodo.</p> <p>Nota: Un nodo puede aparecer como Desconocido durante las operaciones de cierre administradas. Puede ignorar el estado Desconocido en estos casos.</p> |
| | <p>No conectado - administrativamente abajo</p> <p>Por un motivo esperado, el nodo no está conectado a la cuadrícula.</p> <p>Por ejemplo, el nodo o los servicios del nodo se han apagado correctamente, el nodo se está reiniciando o se está actualizando el software. Una o más alertas también pueden estar activas.</p> <p>En función del problema subyacente, estos nodos suelen volver a estar en línea sin ninguna intervención.</p> | <p>Determine si alguna alerta afecta a este nodo.</p> <p>Si hay una o más alertas activas, seleccione cada alerta siga las acciones recomendadas.</p> |
| | <p>Conectado</p> <p>El nodo está conectado a la cuadrícula.</p> | No se requiere ninguna acción. |

Ver las alertas actuales y resueltas

Alertas actuales: Cuando se activa una alerta, se muestra un ícono de alerta en el panel de control. También se muestra un ícono de alerta para el nodo en la página Nodes. If "las notificaciones por correo electrónico de alertas están configuradas", también se enviará una notificación por correo electrónico, a menos que se haya silenciado la alerta.

Alertas resueltas: Puedes buscar y ver un historial de alertas que se han resuelto.

Opcionalmente has visto el vídeo:

[Descripción general de alertas](#)

En la siguiente tabla se describe la información que se muestra en Grid Manager para las alertas actuales y resueltas.

| Encabezado de columna | Descripción |
|---|---|
| Nombre o título | El nombre de la alerta y su descripción. |
| Gravedad | <p>La gravedad de la alerta. Para las alertas actuales, si se agrupan varias alertas, la fila de título muestra cuántas instancias de esa alerta se producen en cada gravedad.</p> <p> Crítico: Existe una condición anormal que ha detenido las operaciones normales de un nodo o servicio StorageGRID. Debe abordar el problema subyacente de inmediato. Se pueden producir interrupciones del servicio y pérdida de datos si no se resuelve el problema.</p> <p> Mayor: Existe una condición anormal que está afectando las operaciones actuales o acercándose al umbral de una alerta crítica. Debe investigar las alertas principales y solucionar cualquier problema subyacente para garantizar que esta condición no detenga el funcionamiento normal de un nodo o servicio de StorageGRID.</p> <p> Menor: El sistema funciona normalmente, pero existe una condición anormal que podría afectar la capacidad del sistema para funcionar si continúa. Debe supervisar y resolver alertas menores que no borren por sí solas para asegurarse de que no den lugar a un problema más grave.</p> |
| Tiempo activado | <p>Alertas actuales: La fecha y hora en que se activó la alerta en su hora local y en UTC. Si se agrupan varias alertas, la fila de título muestra las horas de la instancia más reciente de la alerta (<i>Newest</i>) y la instancia más antigua de la alerta (<i>oldest</i>).</p> <p>Alertas resueltas: Hace cuánto tiempo se activó la alerta.</p> |
| Sitio/nodo | El nombre del sitio y del nodo donde se produce o se ha producido la alerta. |
| Estado | Si la alerta está activa, silenciada o resuelta. Si se agrupan varias alertas y se selecciona todas las alertas en la lista desplegable, la fila de título muestra cuántas instancias de esa alerta están activas y cuántas instancias se han silenciado. |
| Tiempo de resolución (solo alertas resueltas) | Hace cuánto tiempo se resolvió la alerta. |

| Encabezado de columna | Descripción |
|---|--|
| Valores actuales o <i>valores de datos</i> | <p>El valor de la métrica que provocó el activación de la alerta. En el caso de algunas alertas, se muestran valores adicionales que le ayudarán a comprender e investigar la alerta. Por ejemplo, los valores mostrados para una alerta almacenamiento de datos de objeto bajo incluyen el porcentaje de espacio en disco utilizado, la cantidad total de espacio en disco y la cantidad de espacio en disco utilizado.</p> <p>Nota: Si se agrupan varias alertas actuales, los valores actuales no se muestran en la fila de título.</p> |
| Valores disparados (solo alertas resueltas) | <p>El valor de la métrica que provocó el activación de la alerta. En el caso de algunas alertas, se muestran valores adicionales que le ayudarán a comprender e investigar la alerta. Por ejemplo, los valores mostrados para una alerta almacenamiento de datos de objeto bajo incluyen el porcentaje de espacio en disco utilizado, la cantidad total de espacio en disco y la cantidad de espacio en disco utilizado.</p> |

Pasos

1. Seleccione el enlace **Alertas actuales** o **Alertas resueltas** para ver una lista de alertas en esas categorías. También puede ver los detalles de una alerta seleccionando **NODOS > NODO > Descripción general** y, a continuación, seleccionando la alerta en la tabla Alertas.

De manera predeterminada, las alertas actuales se muestran del siguiente modo:

- Primero se muestran las alertas activadas más recientemente.
- Se muestran varias alertas del mismo tipo como un grupo.
- No se muestran las alertas silenciadas.
- Para una alerta específica de un nodo específico, si los umbrales se alcanzan para más de una gravedad, solo se muestra la alerta más grave. Es decir, si se alcanzan los umbrales de alerta para las gravedades leve, grave y crítica, solo se muestra la alerta crítica.

La página de alertas actuales se actualiza cada dos minutos.

2. Para expandir grupos de alertas, seleccione el signo de intercalación hacia abajo . Para reducir alertas individuales de un grupo, seleccione el signo de intercalación ascendente o seleccione el nombre del grupo.
3. Para mostrar alertas individuales en lugar de grupos de alertas, desactive la casilla de verificación **Alertas de grupo**.
4. Para ordenar las alertas actuales o los grupos de alertas, seleccione las flechas arriba/abajo en cada encabezado de columna.
 - Cuando se selecciona **Alertas de grupo**, se ordenan tanto los grupos de alertas como las alertas individuales de cada grupo. Por ejemplo, es posible que desee ordenar las alertas de un grupo por **tiempo activado** para encontrar la instancia más reciente de una alerta específica.
 - Cuando se borra **Alertas de grupo**, se ordena toda la lista de alertas. Por ejemplo, es posible que desee ordenar todas las alertas por **nodo/Sitio** para ver todas las alertas que afectan a un nodo específico.
5. Para filtrar las alertas actuales por estado (**Todas las alertas**, **Activa** o **Silenciada**), usa el menú

desplegable en la parte superior de la tabla.

Consulte "[Silenciar notificaciones de alerta](#)".

6. Para ordenar alertas resueltas:

- Seleccione un período de tiempo en el menú desplegable **When Trigger**.
- Seleccione una o más gravedades en el menú desplegable **Gravedad**.
- Seleccione una o más reglas de alerta predeterminadas o personalizadas en el menú desplegable **Regla de alerta** para filtrar las alertas resueltas relacionadas con una regla de alerta específica.
- Seleccione uno o más nodos en el menú desplegable **Node** para filtrar las alertas resueltas relacionadas con un nodo específico.

7. Para ver los detalles de una alerta específica, seleccione la alerta. Un cuadro de diálogo proporciona detalles y acciones recomendadas para la alerta seleccionada.

8. (Opcional) Para una alerta específica, seleccione Silenciar esta alerta para silenciar la regla de alerta que provocó la activación de esta alerta.

Debe tener el "[Gestionar alertas o permisos de acceso raíz](#)" para silenciar una regla de alerta.



Tenga cuidado al decidir silenciar una regla de alerta. Si se silencia una regla de alerta, es posible que no detecte un problema subyacente hasta que impida que se complete una operación crítica.

9. Para ver las condiciones actuales de la regla de alerta:

a. En los detalles de la alerta, selecciona **Ver condiciones**.

Aparece una ventana emergente que muestra la expresión Prometheus de cada gravedad definida.

b. Para cerrar la ventana emergente, haga clic en cualquier lugar fuera de la ventana emergente.

10. Opcionalmente, seleccione **Editar regla** para editar la regla de alerta que provocó que se activara esta alerta.

Debe tener el "[Gestionar alertas o permisos de acceso raíz](#)" para editar una regla de alerta.



Tenga cuidado al decidir editar una regla de alerta. Si cambia los valores de activación, es posible que no detecte un problema subyacente hasta que no se complete una operación crucial.

11. Para cerrar los detalles de la alerta, selecciona **Cerrar**.

Supervise la capacidad de almacenamiento

Supervise el espacio total utilizable disponible para garantizar que el sistema StorageGRID no se quede sin espacio de almacenamiento para objetos o para metadatos de objetos.

StorageGRID almacena datos de objetos y metadatos de objetos por separado y reserva una cantidad específica de espacio para una base de datos Cassandra distribuida que contiene metadatos de objetos. Supervise la cantidad total de espacio consumido por los objetos y los metadatos del objeto, así como las tendencias de la cantidad de espacio consumido por cada uno. Esto le permitirá planificar con antelación la adición de nodos y evitar cualquier interrupción del servicio.

["ver información sobre la capacidad de almacenamiento"](#) Puede establecer el grid completo, para cada sitio y para cada nodo de almacenamiento del sistema StorageGRID.

Supervise la capacidad de almacenamiento de todo el grid

Supervise la capacidad de almacenamiento general del grid para garantizar que quede espacio libre adecuado para los datos de objetos y los metadatos de objetos. Comprender los cambios en la capacidad de almacenamiento a lo largo del tiempo puede ayudarle a añadir nodos de almacenamiento o volúmenes de almacenamiento antes de consumir la capacidad de almacenamiento utilizable del grid.

El panel de Grid Manager le permite evaluar rápidamente la cantidad de almacenamiento disponible para todo el Grid y para cada centro de datos. La página nodos proporciona valores más detallados para los datos de objetos y los metadatos de objetos.

Pasos

1. Evaluar cuánto almacenamiento hay disponible para todo el grid y para cada centro de datos.
 - a. Selecciona **Panel > Descripción general**.
 - b. Observe los valores en el desglose de uso de espacio de datos y en las tarjetas de desglose de uso de espacio permitido por metadatos. Cada tarjeta muestra un porcentaje del uso de almacenamiento, la capacidad del espacio utilizado y el espacio total disponible o permitido por el sitio.



El resumen no incluye medios de archivado.

Data space usage breakdown ⓘ

1.97 MB (0%) of 3.09 TB used overall

| Site name | Data storage usage | Used space | Total space |
|---------------|--------------------|------------|-------------|
| Data Center 3 | 0% | 621.26 KB | 926.62 GB |
| Data Center 1 | 0% | 798.16 KB | 1.24 TB |
| Data Center 2 | 0% | 552.10 KB | 926.62 GB |

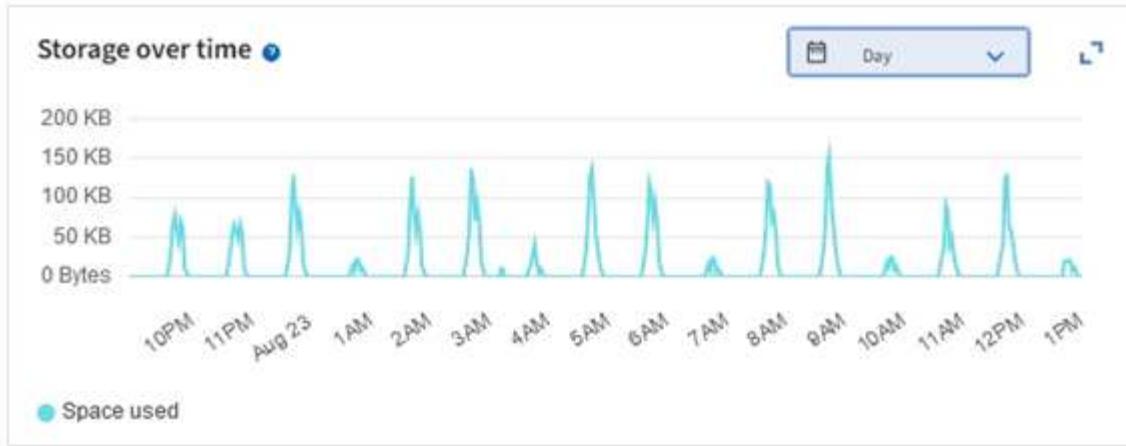
Metadata allowed space usage breakdown ⓘ

2.44 MB (0%) of 19.32 GB used in Data Center 3

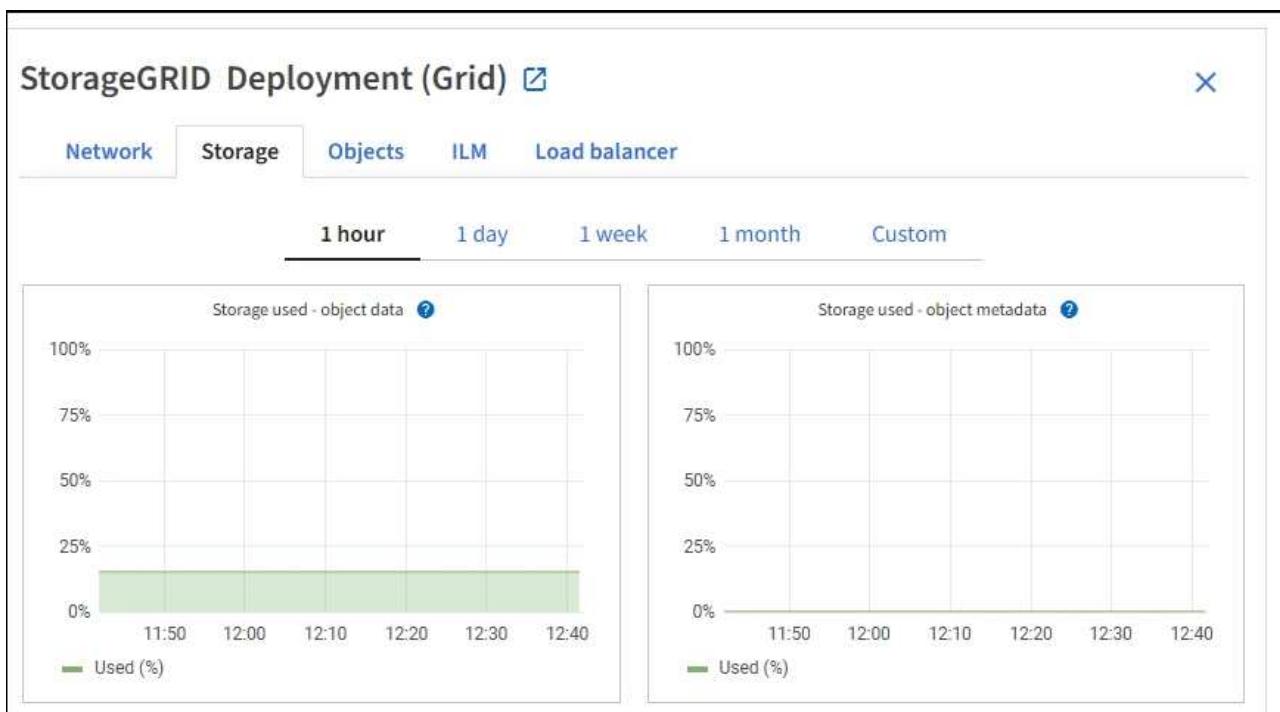
Data Center 3 has the highest metadata space usage and it determines the metadata space available in the grid.

| Site name | Metadata space usage | Metadata used space | Metadata allowed space |
|---------------|----------------------|---------------------|------------------------|
| Data Center 3 | 0% | 2.44 MB | 19.32 GB |

- a. Anote el gráfico en la tarjeta Almacenamiento a lo largo del tiempo. Utilice la lista desplegable Período de tiempo para ayudarle a determinar la rapidez con la que se consume el almacenamiento.



2. Use la página Nodes para obtener más información sobre cuánto almacenamiento se ha usado y cuánto almacenamiento sigue disponible en el grid para datos de objetos y metadatos de objetos.
 - a. Seleccionar **Nodos**.
 - b. Seleccione **grid > almacenamiento**.



- c. Coloque el cursor sobre los gráficos **Almacenamiento usado - datos de objetos** y **Almacenamiento usado - metadatos de objetos** para ver cuánto almacenamiento de objetos y almacenamiento de metadatos de objetos está disponible para toda la cuadrícula, y cuánto se ha utilizado con el tiempo.



Los valores totales de un sitio o de la cuadrícula no incluyen nodos que no hayan informado de métricas durante al menos cinco minutos, como los nodos sin conexión.

3. Planifique realizar una ampliación para añadir nodos de almacenamiento o volúmenes de almacenamiento antes de consumir la capacidad de almacenamiento utilizable del grid.

Al planificar los plazos de una expansión, tenga en cuenta cuánto tiempo se necesitará para adquirir e instalar almacenamiento adicional.



Si su política de ILM utiliza la codificación de borrado, quizás prefiera ampliar cuando los nodos de almacenamiento existentes estén aproximadamente un 70 % llenos para reducir el número de nodos que debe añadirse.

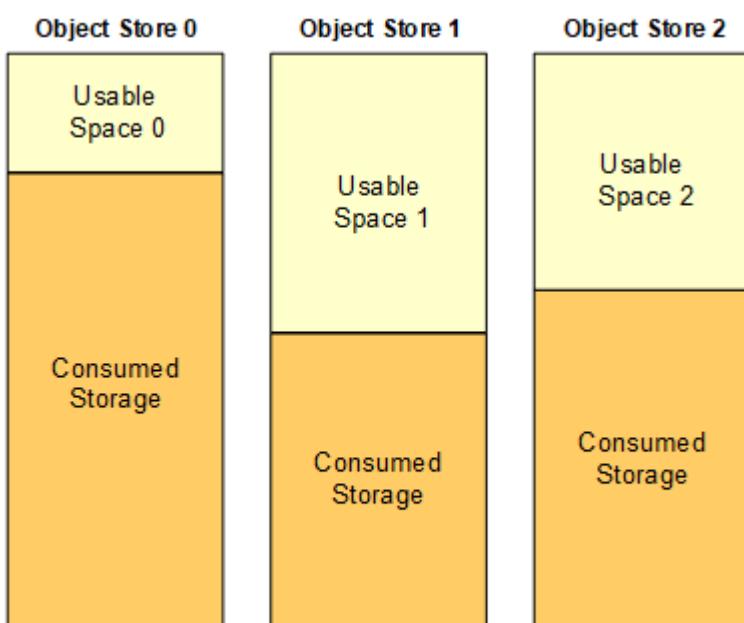
Para obtener más información sobre la planificación de una expansión de almacenamiento, consulte la "[Instrucciones para ampliar StorageGRID](#)".

Supervise la capacidad de almacenamiento para cada nodo de almacenamiento

Supervise el espacio utilizable total de cada nodo de almacenamiento para garantizar que el nodo tenga suficiente espacio para los datos de objetos nuevos.

Acerca de esta tarea

El espacio útil es la cantidad de espacio de almacenamiento disponible para almacenar objetos. El espacio útil total de un nodo de almacenamiento se calcula sumando el espacio disponible en todos los almacenes de objetos del nodo.



$$\text{Total Usable Space} = \text{Usable Space 0} + \text{Usable Space 1} + \text{Usable Space 2}$$

Pasos

1. Seleccione **Nodos > Nodo de almacenamiento > Almacenamiento**.

Aparecen los gráficos y las tablas del nodo.

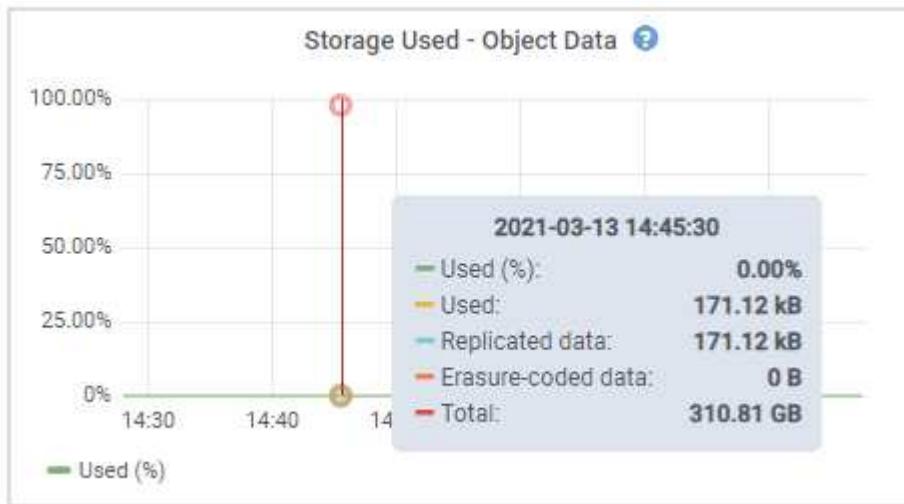
2. Coloque el cursor sobre el gráfico de datos de objetos Storage Used.

Se muestran los siguientes valores:

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

borrado en este nodo, sitio o cuadrícula.

- **Total:** La cantidad total de espacio utilizable en este nodo, sitio o cuadrícula. El valor utilizado es storagegrid_storage_utilization_data_bytes la métrica.



3. Revise los valores disponibles en las tablas Volumes y Object store, debajo de los gráficos.



Para ver gráficos de estos valores, haga clic en los iconos del gráfico en las columnas disponibles.

| Disk devices | | | | | |
|-----------------|-----------------|----------|-----------|------------|--|
| Name | World Wide Name | I/O load | Read rate | Write rate | |
| croot(8:1,sda1) | N/A | 0.04% | 0 bytes/s | 3 KB/s | |
| cvloc(8:2,sda2) | N/A | 0.67% | 0 bytes/s | 50 KB/s | |
| sdc(8:16,sdb) | N/A | 0.03% | 0 bytes/s | 4 KB/s | |
| sdd(8:32,sdc) | N/A | 0.00% | 0 bytes/s | 82 bytes/s | |
| sde(8:48,sdd) | N/A | 0.00% | 0 bytes/s | 82 bytes/s | |

| Volumes | | | | | |
|----------------------|--------|--------|-----------|-----------|--------------------|
| Mount point | Device | Status | Size | Available | Write cache status |
| / | croot | Online | 21.00 GB | 14.75 GB | Unknown |
| /var/local | cvloc | Online | 85.86 GB | 84.05 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 |

| Object stores | | | | | | |
|---------------|-----------|-----------|-----------------|---------|-----------------|-----------|
| ID | Size | Available | Replicated data | EC data | Object data (%) | Health |
| 0000 | 107.32 GB | 96.44 GB | 124.60 KB | 0 bytes | 0.00% | No Errors |
| 0001 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |
| 0002 | 107.32 GB | 107.18 GB | 0 bytes | 0 bytes | 0.00% | No Errors |

- Supervise los valores a lo largo del tiempo para estimar la tasa a la que se está consumiendo el espacio de almacenamiento útil.
- Para mantener las operaciones del sistema normales, añada nodos de almacenamiento, añada volúmenes de almacenamiento o datos de objetos de archivado antes de consumir el espacio útil.

Al planificar los plazos de una expansión, tenga en cuenta cuánto tiempo se necesitará para adquirir e instalar almacenamiento adicional.



Si su política de ILM utiliza la codificación de borrado, quizás prefiera ampliar cuando los nodos de almacenamiento existentes estén aproximadamente un 70 % llenos para reducir el número de nodos que debe añadirse.

Para obtener más información sobre la planificación de una expansión de almacenamiento, consulte la

"Instrucciones para ampliar StorageGRID".

"Almacenamiento de objetos bajo" La alerta se activa cuando queda espacio insuficiente para almacenar datos de objeto en un nodo de almacenamiento.

Supervise la capacidad de metadatos de los objetos para cada nodo de almacenamiento

Supervisar el uso de metadatos de cada nodo de almacenamiento para garantizar que sigue estando disponible un espacio adecuado para las operaciones esenciales de la base de datos. Es necesario añadir nodos de almacenamiento nuevos en cada sitio antes de que los metadatos del objeto superen el 100 % del espacio de metadatos permitido.

Acerca de esta tarea

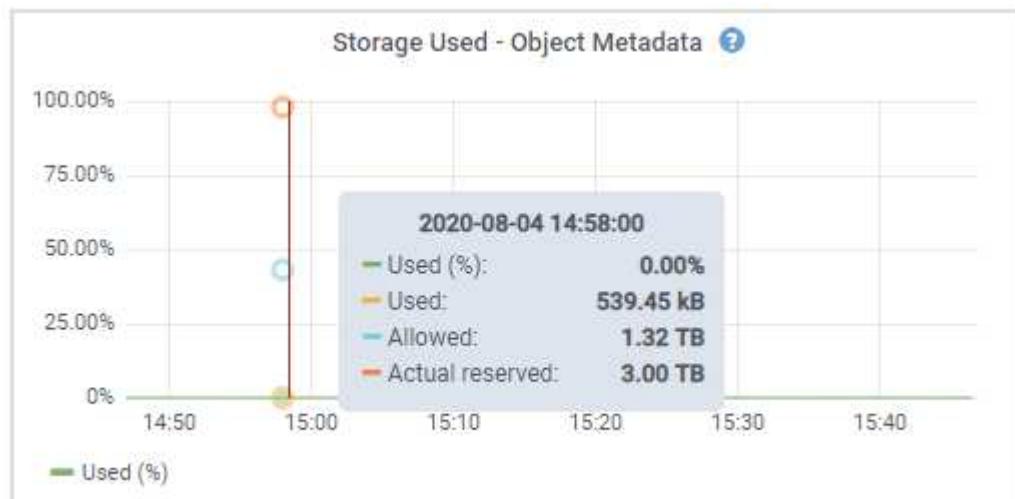
StorageGRID mantiene tres copias de metadatos de objetos en cada sitio para proporcionar redundancia y proteger los metadatos de objetos de la pérdida. Las tres copias se distribuyen uniformemente por todos los nodos de almacenamiento de cada sitio, utilizando el espacio reservado para los metadatos en el volumen de almacenamiento 0 de cada nodo de almacenamiento.

En algunos casos, la capacidad de metadatos de objetos del grid puede consumirse con mayor rapidez que la capacidad de almacenamiento de objetos. Por ejemplo, si normalmente ingiere grandes cantidades de objetos pequeños, es posible que deba añadir nodos de almacenamiento para aumentar la capacidad de metadatos aunque siga habiendo suficiente capacidad de almacenamiento de objetos.

Algunos de los factores que pueden aumentar el uso de metadatos son el tamaño y la cantidad de metadatos y etiquetas de usuario, el número total de partes en una carga de varias partes y la frecuencia de los cambios en las ubicaciones de almacenamiento de ILM.

Pasos

1. Seleccione **Nodos > Nodo de almacenamiento > Almacenamiento**.
2. Coloque el cursor sobre el gráfico de metadatos de objetos Storage Used para ver los valores de un tiempo específico.



Utilizado (%)

El porcentaje de espacio de metadatos permitido que se utilizó en este nodo de almacenamiento.

Métricas de Prometheus: `storagegrid_storage_utilization_metadata_bytes` Y `storagegrid_storage_utilization_metadata_allowed_bytes`

Utilizado

Los bytes del espacio de metadatos permitido que se usaron en este nodo de almacenamiento.

Métrica Prometheus: storagegrid_storage_utilization_metadata_bytes

Permitido

El espacio permitido para los metadatos de objetos en este nodo de almacenamiento. Para obtener más información sobre cómo se determina este valor para cada nodo de almacenamiento, consulte la "[Descripción completa del espacio de metadatos permitido](#)".

Métrica Prometheus: storagegrid_storage_utilization_metadata_allowed_bytes

Reservado real

El espacio real reservado para los metadatos en este nodo de almacenamiento. Incluye el espacio permitido y el espacio necesario para las operaciones esenciales de metadatos. Para obtener más información sobre cómo se calcula este valor para cada nodo de almacenamiento, consulte la "[Descripción completa del espacio reservado real para los metadatos](#)".

La métrica *Prometheus* se añadirá en una versión futura.



Los valores totales de un sitio o de la cuadrícula no incluyen nodos que no hayan informado de métricas durante al menos cinco minutos, como los nodos sin conexión.

- Si el valor **usado (%)** es 70% o superior, expanda su sistema StorageGRID añadiendo nodos de almacenamiento a cada sitio.



La alerta **almacenamiento de metadatos bajo** se activa cuando el valor **usado (%)** alcanza ciertos umbrales. Los resultados no deseables se pueden producir si los metadatos de objetos utilizan más del 100% del espacio permitido.

Cuando se añaden los nodos nuevos, el sistema reequilibra automáticamente los metadatos de objetos en todos los nodos de almacenamiento del sitio. Consulte la "[Instrucciones para ampliar un sistema StorageGRID](#)".

Controla las previsiones de uso de espacio

Supervise las previsiones de uso de espacio para los datos de usuario y los metadatos para estimar cuándo necesitará "[expanda una cuadrícula](#)".

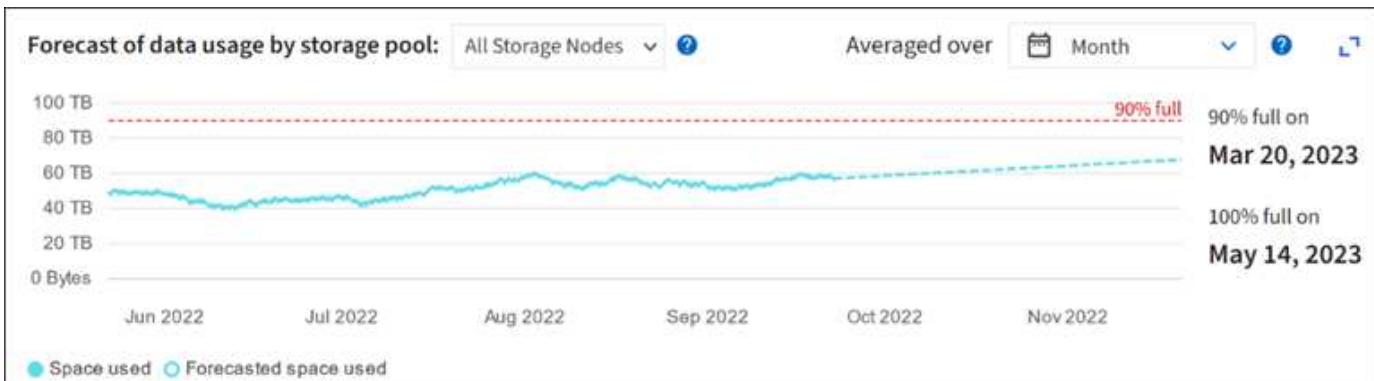
Si observa que la tasa de consumo cambia con el tiempo, seleccione un intervalo más corto del menú desplegable **Promediado sobre** para reflejar solo los patrones de ingesta más recientes. Si observa patrones estacionales, seleccione un rango más largo.

Si tiene una nueva instalación de StorageGRID, permita que los datos y los metadatos se acumulen antes de evaluar las previsiones de uso de espacio.

Pasos

- En el panel de control, seleccione **Almacenamiento**.
- Vea las tarjetas de consolas, Previsión de uso de datos por pool de almacenamiento y Previsión de uso de metadatos por sitio.
- Utilice estos valores para estimar cuándo tendrá que añadir nuevos nodos de almacenamiento para el

almacenamiento de datos y metadatos.



Supervise la gestión del ciclo de vida de la información

El sistema de gestión del ciclo de vida de la información (ILM) proporciona gestión de datos para todos los objetos almacenados en el grid. Debe supervisar las operaciones de ILM para averiguar si el grid puede manejar la carga actual o si se necesitan más recursos.

Acerca de esta tarea

El sistema StorageGRID gestiona los objetos aplicando las políticas de ILM activas. Las políticas de ILM y las reglas de ILM asociadas determinan cuántas copias se realizan, el tipo de copias que se crean, el lugar donde se ubican las copias y el lapso de tiempo que se conserva cada copia.

La ingestión de objetos y otras actividades relacionadas con objetos pueden superar la velocidad a la que StorageGRID puede evaluar el ILM, lo que hace que el sistema ponga en la cola de objetos cuyas instrucciones de ubicación de ILM no se puedan completar prácticamente en tiempo real. Debe supervisar si StorageGRID sigue el ritmo de las acciones del cliente.

Utilizar el separador del panel de control de Grid Manager

Pasos

Utilice la pestaña ILM en el panel de Grid Manager para supervisar las operaciones de ILM:

1. Inicie sesión en Grid Manager.
2. En la consola, seleccione la pestaña ILM y tenga en cuenta los valores de la tarjeta de la cola de ILM (objetos) y la tarjeta de la tasa de evaluación de ILM.

Se esperan picos temporales en la tarjeta de cola de ILM (objetos) en la consola. Sin embargo, si la cola sigue aumentando y en nunca se reduce, el grid necesita más recursos para funcionar de forma eficiente: O bien más nodos de almacenamiento o, si la política de ILM coloca objetos en ubicaciones remotas, más ancho de banda de red.

Utilice la página Nodos

Pasos

Además, investigue las colas de ILM utilizando la página **Nodos**:



Los gráficos en la página **Nodos** se reemplazarán con las tarjetas del panel correspondientes en una futura versión de StorageGRID .

1. Seleccionar **Nodos**.
2. Seleccione **grid name > ILM**.
3. Coloque el cursor sobre el gráfico de cola de ILM para ver el valor de los siguientes atributos en un momento dado:
 - **Objetos en cola (desde operaciones de cliente)**: El número total de objetos que esperan la evaluación de ILM debido a operaciones de cliente (por ejemplo, procesamiento).
 - **Objetos en cola (de todas las operaciones)**: El número total de objetos que esperan la evaluación de ILM.
 - **Velocidad de exploración (objetos/seg.)**: Velocidad a la que se escanean los objetos de la cuadrícula y se colocan en cola para ILM.
 - **Tasa de evaluación (objetos/s)**: La velocidad actual a la que se evalúan los objetos en comparación con la política ILM de la cuadrícula.



La sección de la cola de ILM se incluye solo para el grid. Esta información no se muestra en la pestaña ILM para un sitio o nodo de almacenamiento.

4. En la sección ILM Queue, observe los siguientes atributos.

- **Período de escaneo - Estimado**: El tiempo estimado para completar una exploración completa de ILM de todos los objetos.



Un análisis completo no garantiza que se haya aplicado ILM a todos los objetos.

- **Reparaciones intentadas**: El número total de operaciones de reparación de objetos para los datos replicados que se han intentado. Este número aumenta cada vez que un nodo de almacenamiento intenta reparar un objeto de riesgo alto. Si el Grid está ocupado, se da prioridad a las reparaciones de ILM de alto riesgo.

La misma reparación del objeto podría incrementarse nuevamente si la replicación falla después de la reparación. + Estos atributos pueden ser útiles cuando supervisa el progreso de la recuperación del volumen del nodo de almacenamiento. Si el número de reparaciones intentadas ha dejado de aumentar y se ha completado un análisis completo, es probable que la reparación se haya completado.

5. Alternativamente, envíe una consulta de Prometheus para
`storagegrid_ilm_scan_period_estimated_minutes` y
`storagegrid_ilm_repairs_attempted`.

Supervise las redes y los recursos del sistema

La integridad y el ancho de banda de la red entre nodos y los sitios, y el uso de recursos por parte de los nodos de grid individuales, son esenciales para la eficacia de las operaciones.

Supervisar las conexiones de red y el rendimiento

La conectividad de red y el ancho de banda son especialmente importantes si la política de gestión del ciclo de vida de la información (ILM) copia los objetos replicados entre sitios o almacena objetos codificados con borrado mediante un esquema que proporciona protección contra pérdida de sitio. Si la red entre sitios no está disponible, la latencia de la red es demasiado alta o el ancho de banda de la red es insuficiente, es posible que algunas reglas de ILM no puedan colocar objetos donde se espera. Esto puede provocar errores de

ingesta (cuando se selecciona la opción de ingesta estricta para reglas de ILM) o errores en el rendimiento de procesamiento y los trabajos de gestión de la vida útil.

Utilice Grid Manager para supervisar la conectividad y el rendimiento de la red, de modo que pueda resolver cualquier problema con prontitud.

Además, tenga en cuenta ["creación de políticas de clasificación del tráfico de red"](#) que puede supervisar el tráfico relacionado con inquilinos, depósitos, subredes o extremos de equilibrio de carga específicos. Puede definir políticas de limitación de tráfico según sea necesario.

Pasos

1. Seleccionar Nodos.

Aparece la página Nodes. Cada nodo de la cuadrícula se muestra en formato de tabla.

| Name | Type | Object data used | Object metadata used | CPU usage |
|------------------------|--------------------|------------------|----------------------|-----------|
| StorageGRID Deployment | Grid | 0% | 0% | — |
| Data Center 1 | Site | 0% | 0% | — |
| DC1-ADM1 | Primary Admin Node | — | — | 21% |
| DC1-ARC1 | Archive Node | — | — | 8% |
| DC1-G1 | Gateway Node | — | — | 10% |
| DC1-S1 | Storage Node | 0% | 0% | 29% |

2. Seleccione el nombre de la cuadrícula, un sitio específico del centro de datos o un nodo de la cuadrícula y, a continuación, seleccione la ficha Red.

El gráfico de tráfico de red proporciona un resumen del tráfico general de red para la cuadrícula en su conjunto, el sitio del centro de datos o para el nodo.



- a. Si ha seleccionado un nodo de cuadrícula, desplácese hacia abajo para revisar la sección **interfaces de red** de la página.

| Network interfaces | | | | | |
|--------------------|-------------------|------------|--------|------------------|-------------|
| Name | Hardware address | Speed | Duplex | Auto-negotiation | Link status |
| eth0 | 00:50:56:A7:66:75 | 10 Gigabit | Full | Off | Up |

- b. Para nodos de cuadrícula, desplácese hacia abajo para revisar la sección **Comunicación de red** de la página.

Las tablas de recepción y transmisión muestran cuántos bytes y paquetes se han recibido y enviado a través de cada red, así como otras métricas de recepción y transmisión.

| Network communication | | | | | | | |
|-----------------------|---------|------------|--------|---------|----------------|---------|--|
| Receive | | | | | | | |
| Interface | Data | Packets | Errors | Dropped | Frame overruns | Frames | |
| eth0 | 2.89 GB | 19,421,503 | 0 | 24,032 | 0 | 0 | |
| Transmit | | | | | | | |
| Interface | Data | Packets | Errors | Dropped | Collisions | Carrier | |
| eth0 | 3.64 GB | 18,494,381 | 0 | 0 | 0 | 0 | |

3. Utilice las métricas asociadas a las directivas de clasificación del tráfico para supervisar el tráfico de red.

- a. Seleccione **Configuración > Red > Clasificación de tráfico**.

Aparece la página Directivas de clasificación del tráfico y las directivas existentes se muestran en la

tabla.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.



| Create Edit Remove Metrics | | |
|--|----------------------------------|--------------------------------------|
| Name | Description | ID |
| ERP Traffic Control | Manage ERP traffic into the grid | cd9afbc7-b85e-4208-b6f8-7e8a79e2c574 |
| Fabric Pools | Monitor Fabric Pools | 223b0ccb-6968-4646-b32d-7665bddc894b |

Displaying 2 traffic classification policies.

- Para ver gráficos que muestran las métricas de red asociadas a una directiva, seleccione el botón de opción situado a la izquierda de la directiva y, a continuación, haga clic en **métricas**.
- Revise los gráficos para comprender el tráfico de red asociado a la directiva.

Si una directiva de clasificación de tráfico está diseñada para limitar el tráfico de red, analice la frecuencia con la que el tráfico es limitado y decida si la directiva continúa satisfaciendo sus necesidades. De vez en cuando, ["ajuste cada política de clasificación de tráfico según sea necesario"](#).

Información relacionada

- ["Abra la pestaña Network"](#)
- ["Supervise los estados de conexión de los nodos"](#)

Supervise los recursos a nivel de nodo

Supervisar nodos de cuadrícula individuales para comprobar sus niveles de uso de recursos. Si los nodos están sobrecargados de forma continua, es posible que se necesiten más nodos para realizar operaciones eficientes.

Pasos

- Desde la página **Nodos**, seleccione el nodo.
- Seleccione la ficha **hardware** para visualizar gráficos de utilización de CPU y uso de memoria.



3. Para mostrar un intervalo de tiempo diferente, seleccione uno de los controles situados encima del gráfico o gráfico. Puede visualizar la información disponible para intervalos de 1 hora, 1 día, 1 semana o 1 mes. También puede establecer un intervalo personalizado, que le permite especificar intervalos de fecha y hora.
4. Si el nodo está alojado en un dispositivo de almacenamiento o un dispositivo de servicios, desplácese hacia abajo para ver las tablas de los componentes. El estado de todos los componentes debe ser «Nominal». Investigue los componentes que tienen otro estado.

Información relacionada

- ["Ver información sobre los nodos de almacenamiento de dispositivos"](#)
- ["Consulte información sobre los nodos de administración del dispositivo y los nodos de puerta de enlace"](#)

Supervise la actividad de los inquilinos

Toda la actividad de los clientes de S3 se asocia con las cuentas de inquilino de StorageGRID. Puede usar Grid Manager para supervisar el uso del almacenamiento o el tráfico de red de todos los inquilinos o de un inquilino específico. Puede utilizar el registro de auditoría o los paneles de Grafana para recopilar información más detallada sobre cómo usan los inquilinos StorageGRID.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una ["navegador web compatible"](#).
- Usted tiene el ["Acceso raíz o cuentas de inquilino"](#).

Ver todos los inquilinos

La página Tenedores muestra información básica para todas las cuentas de arrendatario actuales.

Pasos

1. Seleccione **Inquilinos**.

2. Revise la información que se muestra en las páginas de arrendatario.

El espacio lógico utilizado, el uso de cuota, la cuota y el recuento de objetos se enumeran para cada inquilino. Si no se establece una cuota para un arrendatario, los campos Uso de cuota y Cuota contienen un guión (—).



El tamaño lógico de todos los objetos que pertenecen a este inquilino incluye cargas multiparte incompletas y en progreso. El tamaño no incluye el espacio físico adicional utilizado para las políticas de ILM. Los valores de espacio utilizado son estimaciones. Estas estimaciones se ven afectadas por el momento de la ingestión, la conectividad de la red y el estado del nodo.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

| <input type="checkbox"/> | Name | Logical space used | Quota utilization | Quota | Object count | Sign in/Copy URL |
|--------------------------|-----------|--------------------|------------------------------------|-----------|--------------|--|
| <input type="checkbox"/> | Tenant 01 | 2.00 GB | <div style="width: 10%;">10%</div> | 20.00 GB | 100 | → Copy |
| <input type="checkbox"/> | Tenant 02 | 85.00 GB | <div style="width: 85%;">85%</div> | 100.00 GB | 500 | → Copy |
| <input type="checkbox"/> | Tenant 03 | 500.00 TB | <div style="width: 50%;">50%</div> | 1.00 PB | 10,000 | → Copy |
| <input type="checkbox"/> | Tenant 04 | 475.00 TB | <div style="width: 95%;">95%</div> | 500.00 TB | 50,000 | → Copy |
| <input type="checkbox"/> | Tenant 05 | 5.00 GB | — | — | 500 | → Copy |

- Opcionalmente, inicie sesión en una cuenta de inquilino seleccionando el enlace de inicio de sesión → en la columna **Iniciar sesión/Copiar URL**.
- Opcionalmente, copie la URL de la página de inicio de sesión de un inquilino seleccionando el enlace de copia URL [Copy](#) en la columna **Iniciar sesión/Copiar URL**.
- Opcionalmente, seleccione **Exportar a CSV** para ver y exportar un .csv archivo que contiene los valores de uso para todos los inquilinos.

Se le pedirá que abra o guarde el .csv archivo.

El contenido del .csv archivo se parece al siguiente ejemplo:

| Tenant ID | Display Name | Space Used (Bytes) | Quota utilization (%) | Quota (Bytes) | Object Count | Protocol |
|----------------------|--------------|--------------------|-----------------------|---------------|--------------|----------|
| 12659822378459233654 | Tenant 01 | 2000000000 | 10 | 20000000000 | 100 | S3 |
| 99658234112547853685 | Tenant 02 | 85000000000 | 85 | 110000000 | 500 | S3 |
| 03521145586975586321 | Tenant 03 | 60500000000 | 50 | 150000 | 10000 | S3 |
| 44251365987569885632 | Tenant 04 | 47500000000 | 95 | 1400000000 | 50000 | S3 |
| 36521587546689565123 | Tenant 05 | 50000000000 | Infinity | | 500 | S3 |

Puede abrir .csv el archivo en una aplicación de hoja de cálculo o utilizarlo en la automatización.

- Si no se muestra ningún objeto, opcionalmente, seleccione **Acciones > Eliminar** para eliminar uno o más

inquilinos. Consulte "[Eliminar cuenta de inquilino](#)".

No puede eliminar una cuenta de inquilino si la cuenta incluye depósitos o contenedores.

Ver un arrendatario específico

Puede ver los detalles de un arrendatario específico.

Pasos

1. Seleccione el nombre del arrendatario en la página Inquilinos.

Aparece la página de detalles del arrendatario.

The screenshot shows the 'Tenant 02' details page. At the top, it displays general information: Tenant ID (4103 1879 2208 5551 2180), Protocol (S3), Object count (500), Quota utilization (85%), Logical space used (85.00 GB), and Quota (100.00 GB). Below this are three buttons: 'Sign in' (blue), 'Edit' (white), and 'Actions ▾'. Underneath, there are two tabs: 'Space breakdown' (selected) and 'Allowed features'. The 'Space breakdown' section shows a bar chart titled 'Bucket space consumption' with a total of 85.00 GB used out of 100.00 GB, with 15.00 GB remaining (15%). The chart includes a legend for buckets: bucket-01 (light blue), bucket-02 (medium blue), and bucket-03 (dark blue). The 'Bucket details' section shows a table with three rows for buckets: bucket-01, bucket-02, and bucket-03. The columns are Name, Region, Space used, and Object count. The table includes sorting icons for each column.

| Name | Region | Space used | Object count |
|-----------|--------|------------|--------------|
| bucket-01 | | 40.00 GB | 250 |
| bucket-02 | | 30.00 GB | 200 |
| bucket-03 | | 15.00 GB | 50 |

2. Revise la información general del inquilino en la parte superior de la página.

En esta sección de la página de detalles se proporciona información de resumen para el inquilino, incluido el recuento de objetos del inquilino, el uso de la cuota, el espacio lógico utilizado y la configuración de la cuota.



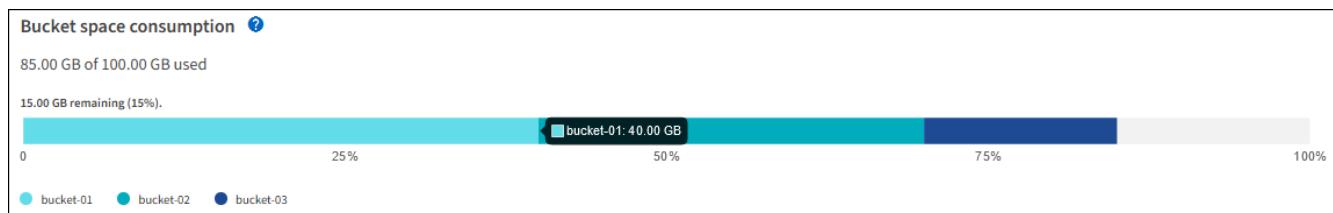
El tamaño lógico de todos los objetos que pertenecen a este inquilino incluye cargas multiparte incompletas y en progreso. El tamaño no incluye el espacio físico adicional utilizado para las políticas de ILM. Los valores de espacio utilizado son estimaciones. Estas estimaciones se ven afectadas por el momento de la ingesta, la conectividad de la red y el estado del nodo.

3. Desde la pestaña **Desglose del espacio**, revisa el gráfico **Consumo de espacio**.

Este gráfico muestra el consumo de espacio total para todos los bloques de S3 del inquilino.

Si se ha establecido una cuota para este arrendatario, la cantidad de cuota utilizada y restante se muestra en texto (por ejemplo, 85.00 GB of 100 GB used). Si no se ha establecido ninguna cuota, el arrendatario tiene una cuota ilimitada y el texto sólo incluye una cantidad de espacio utilizado (por ejemplo, 85.00 GB used). El gráfico de barras muestra el porcentaje de cuota de cada segmento o contenedor. Si el inquilino ha superado la cuota de almacenamiento en más de un 1% y en al menos 1 GB, el gráfico muestra la cuota total y el exceso.

Puede colocar el cursor sobre el gráfico de barras para ver el almacenamiento que utiliza cada cucharón o contenedor. Puede colocar el cursor sobre el segmento de espacio libre para ver la cantidad de cuota de almacenamiento restante.



El uso de la cuota se basa en estimaciones internas y puede superarse en algunos casos. Por ejemplo, StorageGRID comprueba la cuota cuando un inquilino comienza a cargar objetos y rechaza nuevas búsquedas si el inquilino ha superado la cuota. Sin embargo, StorageGRID no tiene en cuenta el tamaño de la carga actual al determinar si se ha superado la cuota. Si se eliminan objetos, se puede evitar temporalmente que un arrendatario cargue nuevos objetos hasta que se vuelva a calcular el uso de cuota. Los cálculos de uso de cuotas pueden tardar 10 minutos o más.



El uso de cuota de un inquilino indica la cantidad total de datos de objeto que el inquilino ha cargado en StorageGRID (tamaño lógico). El uso de cuota no representa el espacio utilizado para almacenar copias de dichos objetos y sus metadatos (tamaño físico).



Puede habilitar la regla de alerta **Uso de cuota de inquilino alto** para determinar si los inquilinos están consumiendo sus cuotas. Si está habilitada, esta alerta se activa cuando un inquilino ha utilizado el 90% de su cuota. Para obtener instrucciones, consulte "["Editar reglas de alerta"](#)".

4. Desde la pestaña **Desglose del espacio**, revisa los detalles de **Bucket**.

En esta tabla se muestran los bloques S3 para el arrendatario. El espacio usado es la cantidad total de datos de objetos en el bloque o contenedor. Este valor no representa el espacio de almacenamiento necesario para las copias de ILM y los metadatos de objetos.

5. Opcionalmente, seleccione **Exportar a CSV** para ver y exportar un archivo .csv que contenga los valores de uso para cada contenedor o bloque.

El contenido de un archivo de un inquilino S3 individual .csv se parece al siguiente ejemplo:

| Tenant ID | Bucket Name | Space Used (Bytes) | Number of Objects |
|----------------------|-------------|--------------------|-------------------|
| 64796966429038923647 | bucket-01 | 88717711 | 14 |
| 64796966429038923647 | bucket-02 | 21747507 | 11 |
| 64796966429038923647 | bucket-03 | 15294070 | 3 |

Puede abrir .csv el archivo en una aplicación de hoja de cálculo o utilizarlo en la automatización.

6. Opcionalmente, seleccione la pestaña **Características permitidas** para ver una lista de los permisos y características que están habilitados para el inquilino. Compruebe "["Edite la cuenta de inquilino"](#)" si necesita cambiar alguno de estos ajustes.
7. Si el inquilino tiene el permiso **Usar conexión de federación de cuadrícula**, opcionalmente seleccione la pestaña **federación de cuadrícula** para obtener más información sobre la conexión.

Consulte "["¿Qué es GRID federation?"](#)" y "["Gestione los inquilinos permitidos para la federación de grid"](#)".

Ver el tráfico de red

Si se han establecido directivas de clasificación de tráfico para un inquilino, revise el tráfico de red para ese arrendatario.

Pasos

1. Seleccione **Configuración > Red > Clasificación de tráfico**.

Aparece la página Directivas de clasificación del tráfico y las directivas existentes se muestran en la tabla.

2. Revise la lista de políticas para identificar las que se aplican a un arrendatario específico.
3. Para ver las métricas asociadas a una política, seleccione el botón de opción situado a la izquierda de la política y seleccione **Métricas**.
4. Analice los gráficos para determinar con qué frecuencia la política limita el tráfico y si necesita ajustar la política.

Consulte "["Administrar directivas de clasificación de tráfico"](#)" para obtener más información.

Use el registro de auditoría

Opcionalmente, se puede utilizar el registro de auditoría para una supervisión más granular de las actividades de un inquilino.

Por ejemplo, puede supervisar los siguientes tipos de información:

- Operaciones específicas del cliente, como PUT, GET o DELETE
- Tamaños de objeto
- La regla de ILM se aplica a los objetos
- La IP de origen de las solicitudes del cliente

Los registros de auditoría se escriben en archivos de texto que se pueden analizar con la herramienta de análisis de registros que elija. Esto le permite comprender mejor las actividades de los clientes o implementar modelos sofisticados de pago por uso y facturación.

Consulte "[Revisar los registros de auditoría](#)" para obtener más información.

Utilizar métricas de Prometheus

Opcionalmente, utilice las métricas de Prometheus para generar informes sobre la actividad del inquilino.

- En el Administrador de cuadrícula, seleccione **Soporte > Herramientas > Métricas**. Puede utilizar paneles existentes, como S3 Overview, para revisar las actividades del cliente.



Las herramientas disponibles en la página Metrics están destinadas principalmente al soporte técnico. Algunas funciones y elementos de menú de estas herramientas no son intencionalmente funcionales.

- En la parte superior de Grid Manager, selecciona el ícono de ayuda y selecciona **Documentación de API**. Puede utilizar las métricas de la sección Métricas de la API de gestión de grid para crear reglas de alerta y paneles personalizados para la actividad de inquilinos.

Consulte "[Revisar las métricas de soporte](#)" para obtener más información.

Supervise las operaciones del cliente S3

Es posible supervisar las tasas de procesamiento y recuperación de objetos, así como las métricas para el número de objetos, consultas y verificación. Puede ver el número de intentos fallidos y correctos por las aplicaciones cliente para leer, escribir y modificar objetos en el sistema StorageGRID.

Antes de empezar

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

Pasos

1. En el panel de control, seleccione la pestaña **Rendimiento**.
2. Consulte los gráficos S3, que resumen la cantidad de operaciones de cliente que realizan los nodos de almacenamiento y la cantidad de solicitudes API que reciben los nodos de almacenamiento durante el lapso seleccionado.
3. Seleccione **Nodos** para acceder a la página Nodos.
4. En la página de inicio de los nodos (nivel de cuadrícula), seleccione la pestaña **Objetos**.

El gráfico muestra las tasas de procesamiento y recuperación de S3 de todo su sistema StorageGRID en bytes por segundo y la cantidad de datos ingeridos o recuperados. Puede seleccionar un intervalo de tiempo o aplicar un intervalo personalizado.

5. Para ver la información de un nodo de almacenamiento en particular, seleccione el nodo de la lista de la izquierda y seleccione la pestaña **Objetos**.

El gráfico muestra las tasas de ingestión y recuperación del nodo. En la pestaña también se incluyen métricas para recuentos de objetos, consultas de metadatos y operaciones de verificación.



Supervisar las operaciones de equilibrio de carga

Si está utilizando un equilibrador de carga para gestionar las conexiones de cliente a StorageGRID, debe supervisar las operaciones de equilibrio de carga después de configurar el sistema inicialmente y después de realizar cualquier cambio de configuración o llevar a cabo una ampliación.

Acerca de esta tarea

Puede usar el servicio Load Balancer en nodos de administración o nodos de pasarela o un equilibrador de carga externo de terceros para distribuir solicitudes de cliente a través de varios nodos de almacenamiento.

Después de configurar el equilibrio de carga, debe confirmar que las operaciones de ingesta y recuperación de objetos se encuentren distribuidas uniformemente en los nodos de almacenamiento. Las solicitudes distribuidas de forma equitativa garantizan que StorageGRID sigue respondiendo a las solicitudes de los clientes bajo carga y pueden ayudar a mantener el rendimiento del cliente.

Si configuró un grupo de alta disponibilidad de nodos de puerta de enlace o nodos de administración en modo de backup activo, solo un nodo del grupo distribuye de forma activa las solicitudes de cliente.

Para obtener más información, consulte "[Configure las conexiones de cliente S3](#)".

Pasos

1. Si los clientes S3 se conectan mediante el servicio de equilibrio de carga, compruebe que los nodos de administración o de puerta de enlace estén distribuyendo el tráfico de forma activa según lo previsto:

- a. Seleccionar **Nodos**.
- b. Seleccione un nodo de puerta de enlace o un nodo de administrador.
- c. En la pestaña **Overview**, compruebe si una interfaz de nodo está en un grupo HA y si la interfaz de nodo tiene el rol Primary.

Los nodos con la función de principal y los nodos que no están en un grupo de alta disponibilidad deberían distribuir solicitudes a los clientes de forma activa.

- d. Para cada nodo que deba distribuir activamente las solicitudes de cliente, seleccione la "[Separador Equilibrador de Carga](#)".
- e. Revise el gráfico de Load Balancer Request Traffic de la última semana para asegurarse de que el nodo ha estado distribuyendo solicitudes de forma activa.

Los nodos de un grupo de alta disponibilidad de backup activo pueden asumir el rol de backup de vez en cuando. Durante ese tiempo, los nodos no distribuyen las solicitudes de los clientes.

- f. Revise el gráfico de la velocidad de solicitud entrante del equilibrador de carga de la última semana para revisar el rendimiento del objeto del nodo.
 - g. Repita estos pasos para cada nodo de administración o nodo de puerta de enlace del sistema StorageGRID.
 - h. Opcionalmente, utilice las políticas de clasificación de tráfico para ver un análisis más detallado del tráfico que presta el servicio de Equilibrador de Carga.
2. Compruebe que estas solicitudes se distribuyen uniformemente en los nodos de almacenamiento.
- a. Seleccione **Storage Node > LDR > HTTP**.
 - b. Revisar el número de **sesiones entrantes actualmente establecidas**.
 - c. Repita esto para cada nodo de almacenamiento de la cuadrícula.

El número de sesiones debe ser aproximadamente igual en todos los nodos de almacenamiento.

Supervisar las conexiones de federación de grid

Puede supervisar la información básica sobre todos "[conexiones de federación de grid](#)", información detallada sobre una conexión específica o las métricas de Prometheus sobre las operaciones de replicación entre redes. Puede supervisar una conexión desde cualquier cuadrícula.

Antes de empezar

- Ha iniciado sesión en Grid Manager en cualquiera de las cuadrículas mediante una "[navegador web compatible](#)".
- Tiene "[Permiso de acceso raíz](#)" el para la cuadrícula en la que ha iniciado sesión.

Ver todas las conexiones

La página de federación de grid muestra información básica sobre todas las conexiones de federación de grid y sobre todas las cuentas de arrendatario que pueden utilizar conexiones de federación de grid.

Pasos

1. Seleccione **Configuración > Sistema > Federación de red**.

Aparecerá la página Grid federation.

2. Para ver la información básica de todas las conexiones en esta cuadrícula, seleccione la pestaña **Conecciones**.

Desde esta pestaña, puede:

- "[Cree una nueva conexión](#)".
- Seleccione una conexión existente a "[editar o probar](#)".

The screenshot shows the 'Grid federation' page with the 'Connections' tab selected. At the top, there's a brief description: 'You can use grid federation to clone tenant accounts and replicate their objects between two StorageGRID systems. Grid federation uses a trusted and secure connection between Admin and Gateway Nodes in two discrete StorageGRID systems.' To the right is a link to 'Learn more about grid federation'. Below the description is a search bar and a table. The table has columns for 'Connection name', 'Remote hostname', and 'Connection status'. One row is visible, showing 'Grid 1 - Grid 2' as the connection name, '10.96.130.76' as the remote hostname, and 'Connected' with a green checkmark as the status.

3. Para ver información básica de todas las cuentas de inquilino en esta cuadrícula que tienen el permiso **Usar conexión de federación de grid**, selecciona la pestaña **Inquilinos permitidos**.

Desde esta pestaña, puede:

- "[Consulte la página de detalles de cada inquilino permitido](#)".
- Consulte la página de detalles de cada conexión. Consulte [Ver una conexión específica](#).
- Seleccione un arrendatario permitido y "[elimine el permiso](#)".
- Compruebe si hay errores de replicación entre cuadrículas y borre el último error, si lo hubiera. Consulte "[Solucionar errores de federación de grid](#)".

Grid federation

[Learn more about grid federation](#)

You can use grid federation to clone tenant accounts and replicate their objects between two StorageGRID systems. Grid federation uses a trusted and secure connection between Admin and Gateway Nodes in two discrete StorageGRID systems.

The screenshot shows a user interface for managing grid federation connections. At the top, there are two tabs: 'Connections' and 'Permitted tenants'. The 'Permitted tenants' tab is selected and highlighted in yellow. Below the tabs are several buttons: 'Remove permission', 'Clear error', and a search bar with placeholder text 'Search...'. To the right of the search bar is a magnifying glass icon. Further to the right, it says 'Displaying one result'. Below these controls is a table header row with columns: 'Tenant name', 'Connection name', 'Connection status', 'Remote grid hostname', and 'Last error'. The table contains one row of data: 'Tenant A' (with a blue circular icon), 'Grid 1 - Grid 2' (with a green checkmark icon), 'Connected' (with a green checkmark icon), '10.96.130.76', and a 'Check for errors' button.

Ver una conexión específica

Puede ver los detalles de una conexión de federación de grid específica.

Pasos

1. Seleccione cualquiera de los separadores de la página federación de Cuadrículas y, a continuación, seleccione el nombre de la conexión en la tabla.

En la página de detalles de la conexión, puede:

- Consulte la información básica sobre el estado de la conexión, incluidos los nombres de host locales y remotos, el puerto y el estado de la conexión.
- Seleccione una conexión a "[editar, probar o eliminar](#)".

2. Cuando vea una conexión específica, seleccione la pestaña **Arrendatarios permitidos** para ver detalles sobre los inquilinos permitidos para la conexión.

Desde esta pestaña, puede:

- ["Consulte la página de detalles de cada inquilino permitido"](#).
- ["Eliminar el permiso de un inquilino"](#) para utilizar la conexión.
- Compruebe si hay errores de replicación entre cuadrículas y borre el último error. Consulte "["Solucionar errores de federación de grid"](#)".

Grid 1 - Grid 2

Local hostname (this grid): 10.96.130.64
Port: 23000
Remote hostname (other grid): 10.96.130.76
Connection status:  Connected

[Edit](#) [Download file](#) [Test connection](#) [Remove](#)

Permitted tenants

Certificates

[Remove permission](#)

[Clear error](#)

Search...



Displaying one result.

Tenant name 

Last error 



Tenant A

[Check for errors](#)

3. Cuando vea una conexión específica, seleccione la pestaña **Certificados** para ver los certificados de servidor y cliente generados por el sistema para esta conexión.

Desde esta pestaña, puede:

- "Rotar certificados de conexión".
- Seleccione **Servidor** o **Cliente** para ver o descargar el certificado asociado o copiar el certificado PEM.

Grid A-Grid B

Local hostname (this grid): 10.96.106.230
Port: 23000
Remote hostname (other grid): 10.96.104.230
Connection status:  Connected

[Edit](#) [Download file](#) [Test connection](#) [Remove](#)

[Permitted tenants](#)

Certificates

[Rotate certificates](#)

[Server](#) [Client](#)

[Download certificate](#)

[Copy certificate PEM](#)

Metadata

Subject DN: /C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=10.96.106.230
Serial number: 30:81:B8:DD:AE:B2:86:0A
Issuer DN: /C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=GPT
Issued on: 2022-10-04T02:21:18.000Z
Expires on: 2024-10-03T19:05:13.000Z
SHA-1 fingerprint: 92:7A:03:AF:6D:1C:94:8C:33:24:08:84:F9:2B:01:23:7D:BE:F2:DF
SHA-256 fingerprint: 54:97:3E:77:EB:D3:6A:0F:8F:EE:72:83:D0:39:86:02:32:A5:60:9D:6F:C0:A2:3C:76:DA:3F:4D:FF:64:5D:60
Alternative names: IP Address:10.96.106.230

Certificate PEM

```
-----BEGIN CERTIFICATE-----  
MIIGdTCCB2gAwIBAgIIMIIG3a6yhgowDQYJKoZIhvvcNAQENBQAwdzELMAkGA1UE  
BhMCVVMxExARBgNVBAgICkNhbg1mb3JuaWExEjAQBgNVBAcMCVN1bm55dmFsZTEU  
MRQFU15CaWtVQ0FUV4vA7eANVBAsMEh1dEF...CB74ggWd1R11
```

Revisión de las métricas de replicación entre grid

Puede utilizar el panel de control de replicación de cuadrícula cruzada en Grafana para ver las métricas de Prometheus sobre las operaciones de replicación entre grid en su grid.

Pasos

1. Desde el Administrador de cuadrícula, seleccione **Soporte > Herramientas > Métricas**.



Las herramientas disponibles en la página Métricas están destinadas al soporte técnico. Algunas funciones y elementos de menú de estas herramientas no son intencionalmente funcionales y están sujetos a cambios. Consulte la lista de "[Métricas de Prometheus que se usan habitualmente](#)".

2. En la sección Grafana de la página, selecciona **Replicación de cuadrícula cruzada**.

Para obtener instrucciones detalladas, consulte "[Revisar las métricas de soporte](#)".

3. Para volver a intentar la replicación de objetos que no se han podido replicar, consulte "["Identifique y vuelva a intentar operaciones de replicación fallidas"](#)".

Gestionar alertas

Gestionar alertas

El sistema de alertas proporciona una interfaz fácil de usar para detectar, evaluar y resolver los problemas que pueden ocurrir durante el funcionamiento de StorageGRID.

Las alertas se activan en niveles de gravedad específicos cuando las condiciones de regla de alerta se evalúan como verdaderas. Cuando se activa una alerta, se realizan las siguientes acciones:

- Se muestra un ícono de gravedad de alerta en el panel de control de Grid Manager y el recuento de alertas actuales se incrementa.
- La alerta se muestra en la página de resumen de **Nodos** y en la pestaña **Nodos > nodo > Descripción general**.
- Se envía una notificación por correo electrónico, suponiendo que se haya configurado un servidor SMTP y que se hayan proporcionado direcciones de correo electrónico para los destinatarios.
- Se envía una notificación de Protocolo simple de administración de red (SNMP), suponiendo que haya configurado el agente SNMP de StorageGRID.

Es posible crear alertas personalizadas, editar o deshabilitar alertas, y gestionar notificaciones de alertas.

Si quiere más información:

- Revisa los videos:

[Descripción general de alertas](#)

[Alertas personalizadas](#)

- Consulte la "[Referencia de alertas](#)" .

Ver reglas de alerta

Las reglas de alerta definen las condiciones que disparan "[alertas específicas](#)".

StorageGRID incluye un conjunto de reglas de alerta predeterminadas, que se pueden utilizar tal cual o modificar, o bien se pueden crear reglas de alerta personalizadas.

Puede ver la lista de todas las reglas de alerta predeterminadas y personalizadas para saber qué condiciones desencadenarán cada alerta y ver si hay alguna alerta desactivada.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Usted tiene el "["Gestionar alertas o permisos de acceso raíz"](#)".
- Opcionalmente has visto el vídeo:

[Descripción general de alertas](#)

Pasos

1. Seleccione Alertas > Reglas.

Aparecerá la página Reglas de alerta.

Alert Rules [Learn more](#)

Alert rules define which conditions trigger specific alerts.

You can edit the conditions for default alert rules to better suit your environment, or create custom alert rules that use your own conditions for triggering alerts.

| + Create custom rule | Edit rule | Remove custom rule | |
|--|--|------------------------------------|---------|
| Name | Conditions | Type | Status |
| Appliance battery expired The battery in the appliance's storage controller has expired. | storagegrid_appliance_component_failure(type="REC_EXPIRED_BATTERY") Major > 0 | Default | Enabled |
| Appliance battery failed The battery in the appliance's storage controller has failed. | storagegrid_appliance_component_failure(type="REC_FAILED_BATTERY") Major > 0 | Default | Enabled |
| Appliance battery has insufficient learned capacity The battery in the appliance's storage controller has insufficient learned capacity. | storagegrid_appliance_component_failure(type="REC_BATTERY_WARN") Major > 0 | Default | Enabled |
| Appliance battery near expiration The battery in the appliance's storage controller is nearing expiration. | storagegrid_appliance_component_failure(type="REC_BATTERY_NEAR_EXPIRATION") Major > 0 | Default | Enabled |
| Appliance battery removed The battery in the appliance's storage controller is missing. | storagegrid_appliance_component_failure(type="REC_REMOVED_BATTERY") Major > 0 | Default | Enabled |
| Appliance battery too hot The battery in the appliance's storage controller is overheated. | storagegrid_appliance_component_failure(type="REC_BATTERY_OVERTEMP") Major > 0 | Default | Enabled |
| Appliance cache backup device failed A persistent cache backup device has failed. | storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_FAILED") Major > 0 | Default | Enabled |
| Appliance cache backup device insufficient capacity There is insufficient cache backup device capacity. | storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY") Major > 0 | Default | Enabled |
| Appliance cache backup device write-protected A cache backup device is write-protected. | storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED") Major > 0 | Default | Enabled |
| Appliance cache memory size mismatch The two controllers in the appliance have different cache sizes. | storagegrid_appliance_component_failure(type="REC_CACHE_MEM_SIZE_MISMATCH") Major > 0 | Default | Enabled |

Displaying 62 alert rules.

2. Revise la información en la tabla de reglas de alertas:

| Encabezado de columna | Descripción |
|-----------------------|---|
| Nombre | El nombre único y la descripción de la regla de alerta. Las reglas de alerta personalizadas se enumeran primero, seguidas de reglas de alerta predeterminadas. El nombre de la regla de alerta es el asunto de las notificaciones por correo electrónico. |

| Encabezado de columna | Descripción |
|-----------------------|--|
| Condiciones | <p>Expresiones Prometheus que determinan cuándo se activa esta alerta. Puede activarse una alerta en uno o más de los siguientes niveles de gravedad, pero no es necesario utilizar una condición para cada gravedad.</p> <ul style="list-style-type: none"> • Crítico : Existe una condición anormal que ha detenido las operaciones normales de un nodo o servicio StorageGRID. Debe abordar el problema subyacente de inmediato. Se pueden producir interrupciones del servicio y pérdida de datos si no se resuelve el problema. • Mayor : Existe una condición anormal que está afectando las operaciones actuales o acercándose al umbral de una alerta crítica. Debe investigar las alertas principales y solucionar cualquier problema subyacente para garantizar que esta condición no detenga el funcionamiento normal de un nodo o servicio de StorageGRID. • Menor : El sistema funciona normalmente, pero existe una condición anormal que podría afectar la capacidad del sistema para funcionar si continúa. Debe supervisar y resolver alertas menores que no borren por sí solas para asegurarse de que no den lugar a un problema más grave. |
| Tipo | <p>Tipo de regla de alerta:</p> <ul style="list-style-type: none"> • Valor predeterminado: Regla de alerta proporcionada con el sistema. Puede deshabilitar una regla de alerta predeterminada o editar las condiciones y la duración de una regla de alerta predeterminada. No puede eliminar una regla de alerta predeterminada. • Predeterminado*: Regla de alerta predeterminada que incluye una condición o duración editada. Según sea necesario, puede revertir fácilmente una condición modificada al valor predeterminado original. • Personalizado: Regla de alerta que ha creado. Puede deshabilitar, editar y eliminar reglas de alerta personalizadas. |
| Estado | <p>Si esta regla de alerta está activada o desactivada. No se evalúan las condiciones para las reglas de alerta desactivadas, por lo que no se activa ninguna alerta.</p> |

Crear reglas de alerta personalizadas

Puede crear reglas de alerta personalizadas para definir sus propias condiciones para activar alertas.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Usted tiene el "[Gestionar alertas o permisos de acceso raíz](#)".
- Usted está familiarizado con el "[Métricas de Prometheus que se usan habitualmente](#)".

- Usted entiende el "[Sintaxis de las consultas Prometheus](#)".
- Opcionalmente has visto el vídeo:

[Alertas personalizadas](#)

Acerca de esta tarea

StorageGRID no valida alertas personalizadas. Si decide crear reglas de alerta personalizadas, siga estas directrices generales:

- Observe las condiciones de las reglas de alerta predeterminadas y utilícela como ejemplos para sus reglas de alerta personalizadas.
- Si define más de una condición para una regla de alerta, utilice la misma expresión para todas las condiciones. A continuación, cambie el valor del umbral para cada condición.
- Compruebe con cuidado cada condición en busca de errores tipográficos y lógicos.
- Utilice sólo las métricas enumeradas en la API de gestión de grid.
- Al probar una expresión con la API de gestión de grid, tenga en cuenta que una respuesta correcta puede ser un cuerpo de respuesta vacío (no se ha activado ninguna alerta). Para ver si la alerta está activada realmente, puede configurar temporalmente un umbral en el valor que espera que sea TRUE actualmente.

Por ejemplo, para probar la expresión `node_memory_MemTotal_bytes < 24000000000`, primero ejecute `node_memory_MemTotal_bytes >= 0` y asegúrese de obtener los resultados esperados (todos los nodos devuelven un valor). A continuación, vuelva a cambiar el operador y el umbral a los valores previstos y vuelva a ejecutarlo. Ningún resultado indica que no hay alertas actuales para esta expresión.

- No asuma que una alerta personalizada funciona a menos que haya validado que la alerta se activa en el momento esperado.

Pasos

1. Seleccione **Alertas > Reglas**.

Aparecerá la página Reglas de alerta.

2. Seleccione **Crear regla personalizada**.

Aparece el cuadro de diálogo Crear regla personalizada.

Create Custom Rule

Enabled

Unique Name

Description

Recommended Actions
(optional)

Conditions

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

 5 minutes ▾

Cancel

Save

3. Active o desactive la casilla de verificación **Enabled** para determinar si esta regla de alerta está actualmente habilitada.

Si una regla de alerta está desactivada, sus expresiones no se evalúan y no se activa ninguna alerta.

4. Introduzca la siguiente información:

| Campo | Descripción |
|------------------|--|
| Nombre exclusivo | Nombre único para esta regla. El nombre de la regla de alerta se muestra en la página Alertas y también es el asunto de las notificaciones por correo electrónico. Los nombres de las reglas de alerta pueden tener entre 1 y 64 caracteres. |

| Campo | Descripción |
|-----------------------|--|
| Descripción | Una descripción del problema que se está produciendo. La descripción es el mensaje de alerta que se muestra en la página Alertas y en las notificaciones por correo electrónico. Las descripciones de las reglas de alerta pueden tener entre 1 y 128 caracteres. |
| Acciones recomendadas | De manera opcional, las acciones recomendadas que se deben realizar cuando se activa esta alerta. Introduzca las acciones recomendadas como texto sin formato (sin códigos de formato). Las acciones recomendadas para las reglas de alerta pueden tener entre 0 y 1,024 caracteres. |

5. En la sección Condiciones, introduzca una expresión Prometheus para uno o más niveles de gravedad de alerta.

Una expresión básica suele ser de la forma:

[metric] [operator] [value]

Las expresiones pueden ser de cualquier longitud, pero aparecen en una sola línea en la interfaz de usuario. Se requiere al menos una expresión.

Esta expresión provoca que se active una alerta si la cantidad de RAM instalada para un nodo es inferior a 24,000,000,000 bytes (24 GB).

`node_memory_MemTotal_bytes < 24000000000`

Para ver las métricas disponibles y probar las expresiones de Prometheus, seleccione el icono de ayuda  y siga el enlace a la sección Métricas de la API de administración de grid.

6. En el campo **duración**, introduzca la cantidad de tiempo que una condición debe permanecer en vigor continuamente antes de que se active la alerta y seleccione una unidad de tiempo.

Para activar una alerta inmediatamente cuando una condición se convierte en verdadera, introduzca **0**. Aumente este valor para evitar que las condiciones temporales activen las alertas.

El valor predeterminado es 5 minutos.

7. Seleccione **Guardar**.

El cuadro de diálogo se cierra y la nueva regla de alerta personalizada aparece en la tabla Reglas de alerta.

Editar reglas de alerta

Puede editar una regla de alerta para cambiar las condiciones de activación, para una regla de alerta personalizada, también puede actualizar el nombre de la regla, la descripción y las acciones recomendadas.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Usted tiene el "[Gestionar alertas o permisos de acceso raíz](#)".

Acerca de esta tarea

Al editar una regla de alerta predeterminada, puede cambiar las condiciones de las alertas menores, principales y críticas, así como la duración. Al editar una regla de alerta personalizada, también puede editar el nombre de la regla, la descripción y las acciones recomendadas.



Tenga cuidado al decidir editar una regla de alerta. Si cambia los valores de activación, es posible que no detecte un problema subyacente hasta que no se complete una operación crucial.

Pasos

1. Seleccione **Alertas > Reglas**.

Aparecerá la página Reglas de alerta.

2. Seleccione el botón de opción de la regla de alerta que desee editar.
3. Seleccione **Editar regla**.

Se muestra el cuadro de diálogo Editar regla. Este ejemplo muestra una regla de alerta predeterminada: Los campos Nombre único, Descripción y Acciones recomendadas están desactivados y no se pueden editar.

Edit Rule - Low installed node memory

| | |
|---|---|
| Enabled | <input checked="" type="checkbox"/> |
| Unique Name | Low installed node memory |
| Description | The amount of installed memory on a node is low. |
| Recommended Actions (optional) | <p>Increase the amount of RAM available to the virtual machine or Linux host. Check the threshold value for the major alert to determine the default minimum requirement for a StorageGRID node.</p> <p>See the instructions for your platform:</p> <ul style="list-style-type: none">• VMware installation• Red Hat Enterprise Linux or CentOS installation• Ubuntu or Debian installation |
| Conditions ? | |
| Minor | |
| Major | node_memory_MemTotal_bytes < 24000000000 |
| Critical | node_memory_MemTotal_bytes <= 12000000000 |
| Enter the amount of time a condition must continuously remain in effect before an alert is triggered. | |
| Duration | 2 minutes ▾ |
| Cancel Save | |

4. Active o desactive la casilla de verificación **Enabled** para determinar si esta regla de alerta está actualmente habilitada.

Si una regla de alerta está desactivada, sus expresiones no se evalúan y no se activa ninguna alerta.



Si deshabilita la regla de alerta para una alerta actual, deberá esperar unos minutos para que la alerta ya no aparezca como alerta activa.



En general, no se recomienda deshabilitar una regla de alerta predeterminada. Si una regla de alerta está deshabilitada, es posible que no se detecte un problema subyacente hasta que no se complete una operación crucial.

5. En el caso de reglas de alerta personalizadas, actualice la siguiente información según sea necesario.



No puede editar esta información para las reglas de alerta predeterminadas.

| Campo | Descripción |
|-----------------------|--|
| Nombre exclusivo | Nombre único para esta regla. El nombre de la regla de alerta se muestra en la página Alertas y también es el asunto de las notificaciones por correo electrónico. Los nombres de las reglas de alerta pueden tener entre 1 y 64 caracteres. |
| Descripción | Una descripción del problema que se está produciendo. La descripción es el mensaje de alerta que se muestra en la página Alertas y en las notificaciones por correo electrónico. Las descripciones de las reglas de alerta pueden tener entre 1 y 128 caracteres. |
| Acciones recomendadas | De manera opcional, las acciones recomendadas que se deben realizar cuando se activa esta alerta. Introduzca las acciones recomendadas como texto sin formato (sin códigos de formato). Las acciones recomendadas para las reglas de alerta pueden tener entre 0 y 1,024 caracteres. |

6. En la sección Condiciones, introduzca o actualice la expresión Prometheus de uno o más niveles de gravedad de alerta.



Si desea restaurar una condición para una regla de alerta predeterminada editada a su valor original, seleccione los tres puntos a la derecha de la condición modificada.

Conditions

| | |
|----------|--|
| Minor | <input type="text"/> |
| Major | <input type="text"/> node_memory_MemTotal_bytes < 24000000000 |
| Critical | <input type="text"/> node_memory_MemTotal_bytes <= 14000000000 |



Si actualiza las condiciones para una alerta actual, es posible que los cambios no se implementen hasta que se resuelva la condición anterior. La próxima vez que se cumpla una de las condiciones de la regla, la alerta reflejará los valores actualizados.

Una expresión básica suele ser de la forma:

[metric] [operator] [value]

Las expresiones pueden ser de cualquier longitud, pero aparecen en una sola línea en la interfaz de usuario. Se requiere al menos una expresión.

Esta expresión provoca que se active una alerta si la cantidad de RAM instalada para un nodo es inferior a 24,000,000,000 bytes (24 GB).

node_memory_MemTotal_bytes < 24000000000

7. En el campo **duración**, introduzca la cantidad de tiempo que una condición debe permanecer en vigor continuamente antes de que se active la alerta y seleccione la unidad de tiempo.

Para activar una alerta inmediatamente cuando una condición se convierte en verdadera, introduzca **0**. Aumente este valor para evitar que las condiciones temporales activen las alertas.

El valor predeterminado es 5 minutos.

8. Seleccione **Guardar**.

Si ha editado una regla de alerta predeterminada, aparecerá **valor predeterminado*** en la columna **Tipo**.

Si ha desactivado una regla de alerta predeterminada o personalizada, **Desactivada** aparece en la columna **Estado**.

Deshabilitar reglas de alerta

Puede cambiar el estado activado/desactivado para una regla de alerta predeterminada o personalizada.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Usted tiene el "[Gestionar alertas o permisos de acceso raíz](#)".

Acerca de esta tarea

Cuando una regla de alerta está desactivada, sus expresiones no se evalúan y no se activa ninguna alerta.



En general, no se recomienda deshabilitar una regla de alerta predeterminada. Si una regla de alerta está deshabilitada, es posible que no se detecte un problema subyacente hasta que no se complete una operación crucial.

Pasos

1. Seleccione **Alertas > Reglas**.

Aparecerá la página Reglas de alerta.

2. Seleccione el botón de opción de la regla de alerta que deseé desactivar o activar.

3. Seleccione **Editar regla**.

Se muestra el cuadro de diálogo Editar regla.

4. Active o desactive la casilla de verificación **Enabled** para determinar si esta regla de alerta está actualmente habilitada.

Si una regla de alerta está desactivada, sus expresiones no se evalúan y no se activa ninguna alerta.



Si deshabilita la regla de alerta para una alerta actual, debe esperar unos minutos para que la alerta ya no se muestre como una alerta activa.

5. Seleccione **Guardar**.

Desactivado aparece en la columna **Estado**.

Quitar reglas de alerta personalizadas

Puede eliminar una regla de alerta personalizada si ya no desea utilizarla.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Usted tiene el "[Gestionar alertas o permisos de acceso raíz](#)".

Pasos

1. Seleccione **Alertas > Reglas**.

Aparecerá la página Reglas de alerta.

2. Seleccione el botón de opción de la regla de alerta personalizada que desee eliminar.

No puede eliminar una regla de alerta predeterminada.

3. Seleccione **Eliminar regla personalizada**.

Se muestra un cuadro de diálogo de confirmación.

4. Seleccione **Aceptar** para eliminar la regla de alerta.

Las instancias activas de la alerta se resolverán en un plazo de 10 minutos.

Permite gestionar notificaciones de alerta

Configure las notificaciones SNMP para las alertas

Si desea que StorageGRID envíe notificaciones SNMP cuando se produzca una alerta, debe habilitar el agente SNMP de StorageGRID y configurar uno o más destinos de capturas.

Puede utilizar la opción **Configuración > Monitoreo > Agente SNMP** en el Administrador de Grid o los puntos finales SNMP de la API de administración de Grid para habilitar y configurar el agente SNMP de StorageGRID . El agente SNMP admite las tres versiones del protocolo SNMP.

Para obtener información sobre cómo configurar el agente SNMP, consulte "[Usar supervisión de SNMP](#)".

Después de configurar el agente SNMP de StorageGRID, se pueden enviar dos tipos de notificaciones condicionadas por eventos:

- Las trampas son notificaciones enviadas por el agente SNMP que no requieren reconocimiento por parte del sistema de gestión. Los traps sirven para notificar al sistema de gestión que algo ha sucedido dentro de StorageGRID, por ejemplo, que se activa una alerta. Las tres versiones de SNMP admiten capturas.
- Las informes son similares a las capturas, pero requieren el reconocimiento del sistema de gestión. Si el agente SNMP no recibe un acuse de recibo en un periodo de tiempo determinado, vuelve a enviar el informe hasta que se reciba un acuse de recibo o se haya alcanzado el valor de reintento máximo. Las informes son compatibles con SNMPv2c y SNMPv3.

Las notificaciones Trap e informe se envían cuando se activa una alerta predeterminada o personalizada en cualquier nivel de gravedad. Para suprimir las notificaciones SNMP de una alerta, debe configurar un silencio para la alerta. Consulte "[Silenciar notificaciones de alerta](#)".

Si la implementación de StorageGRID incluye varios nodos de administración, el nodo de administración principal es el remitente preferido para las notificaciones de alertas, los paquetes de AutoSupport y las capturas SNMP. Si el nodo de administración principal deja de estar disponible, otros nodos de administración envían temporalmente las notificaciones. Consulte "[¿Qué es un nodo de administración?](#)".

Configure notificaciones por correo electrónico para las alertas

Si desea que se envíen notificaciones por correo electrónico cuando se produzcan alertas, debe proporcionar información acerca del servidor SMTP. También debe introducir direcciones de correo electrónico para los destinatarios de las notificaciones de alerta.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Usted tiene el "[Gestionar alertas o permisos de acceso raíz](#)".

Acerca de esta tarea

La configuración de correo electrónico utilizada para las notificaciones de alertas no se utiliza para los paquetes de AutoSupport. Sin embargo, puede utilizar el mismo servidor de correo electrónico para todas las notificaciones.

Si la implementación de StorageGRID incluye varios nodos de administración, el nodo de administración principal es el remitente preferido para las notificaciones de alertas, los paquetes de AutoSupport y las capturas SNMP. Si el nodo de administración principal deja de estar disponible, otros nodos de administración envían temporalmente las notificaciones. Consulte "[¿Qué es un nodo de administración?](#)".

Pasos

1. Seleccione **Alertas > Configuración de correo electrónico**.

Aparece la página Configuración de correo electrónico.

2. Seleccione la casilla de verificación **Activar notificaciones de correo electrónico** para indicar que desea que se envíen correos electrónicos de notificación cuando las alertas alcancen los umbrales configurados.

Aparecen las secciones servidor de correo electrónico (SMTP), Seguridad de la capa de transporte (TLS), direcciones de correo electrónico y Filtros.

3. En la sección servidor de correo electrónico (SMTP), introduzca la información que necesita StorageGRID para acceder al servidor SMTP.

Si el servidor SMTP requiere autenticación, debe introducir tanto un nombre de usuario como una contraseña.

| Campo | Introduzca |
|--------------------|--|
| Servidor de correo | El nombre de dominio completo (FQDN) o la dirección IP del servidor SMTP. |
| Puerto | El puerto utilizado para acceder al servidor SMTP. Debe estar entre 1 y 65535. |

| Campo | Introduzca |
|------------------------------|--|
| Nombre de usuario (opcional) | Si el servidor SMTP requiere autenticación, introduzca el nombre de usuario con el que desea autenticarse. |
| Contraseña (opcional) | Si el servidor SMTP requiere autenticación, introduzca la contraseña con la que desea autenticarse. |

4. En la sección direcciones de correo electrónico, introduzca las direcciones de correo electrónico del remitente y de cada destinatario.
- En **Dirección de correo electrónico del remitente**, especifique una dirección de correo electrónico válida que se utilizará como dirección de para las notificaciones de alerta.
Por ejemplo: storagegrid-alerts@example.com
 - En la sección Recipients, introduzca una dirección de correo electrónico para cada lista de correo electrónico o persona que debería recibir un correo electrónico cuando se produzca una alerta.
Seleccione el icono más para agregar destinatarios.

5. Si se necesita Seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor SMTP, seleccione **requerir TLS** en la sección Seguridad de la capa de transporte (TLS).
- En el campo **Certificado CA**, proporcione el certificado de CA que se utilizará para verificar la identificación del servidor SMTP.
Puede copiar y pegar el contenido en este campo, o seleccione **examinar** y seleccione el archivo.
Debe proporcionar un solo archivo que contenga los certificados de cada entidad de certificación (CA) intermedia. El archivo debe contener cada uno de los archivos de certificado de CA codificados con PEM, concatenados en el orden de la cadena de certificados.
 - Seleccione la casilla de verificación **Enviar certificado de cliente** si su servidor de correo electrónico SMTP requiere que los remitentes de correo electrónico proporcionen certificados de cliente para la autenticación.
Puede copiar y pegar el contenido en este campo, o seleccione **examinar** y seleccione el archivo.
 - En el campo **Certificado de cliente**, proporcione el certificado de cliente codificado con PEM para enviar al servidor SMTP.
Puede copiar y pegar el contenido en este campo, o seleccione **examinar** y seleccione el archivo.



Si necesita editar la configuración del correo electrónico, seleccione el icono de lápiz para actualizar este campo.

6. En la sección Filtros, seleccione qué niveles de gravedad de alerta deberían producir notificaciones por correo electrónico, a menos que se haya silenciado la regla de una alerta específica.

| Gravedad | Descripción |
|-----------------------|---|
| Menor, mayor, crítico | Se envía una notificación por correo electrónico cuando se cumple la condición menor, mayor o crítica de una regla de alerta. |
| Principal, crítico | Se envía una notificación por correo electrónico cuando se cumple la condición principal o crítica de una regla de alerta. No se envían notificaciones para alertas menores. |
| Solo crítico | Solo se envía una notificación por correo electrónico cuando se cumple la condición crítica de una regla de alerta. No se envían notificaciones para alertas menores o mayores. |

7. Cuando esté listo para probar la configuración de correo electrónico, siga estos pasos:

- Seleccione **Enviar correo electrónico de prueba**.

Aparece un mensaje de confirmación que indica que se ha enviado un correo electrónico de prueba.

- Active las casillas de todos los destinatarios de correo electrónico y confirme que se ha recibido un mensaje de correo electrónico de prueba.



Si el correo electrónico no se recibe en unos minutos o si se activa la alerta **error de notificación por correo electrónico**, compruebe la configuración e inténtelo de nuevo.

- Inicie sesión en cualquier otro nodo de administración y envíe un correo electrónico de prueba para verificar la conectividad desde todos los sitios.



Cuando prueba las notificaciones de alerta, debe iniciar sesión en cada nodo de administrador para verificar la conectividad. Esto es en contraste con probar paquetes AutoSupport, donde todos los nodos de administración envían el correo electrónico de prueba.

8. Seleccione **Guardar**.

El envío de un mensaje de correo electrónico de prueba no guarda la configuración. Debe seleccionar **Guardar**.

Se guardará la configuración del correo electrónico.

Información incluida en las notificaciones por correo electrónico de alertas

Una vez configurado el servidor de correo electrónico SMTP, las notificaciones por correo electrónico se envían a los destinatarios designados cuando se activa una alerta, a menos que la regla de alerta se suprima con un silencio. Consulte ["Silenciar notificaciones de alerta"](#).

Las notificaciones por correo electrónico incluyen la siguiente información:

Low object data storage (6 alerts) 1The space available for storing object data is low. 2**Recommended actions** 3

Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes. See the instructions for expanding a StorageGRID system.

DC1-S1-226

| | | |
|-----------------------|------------------------------|---|
| Node | DC1-S1-226 | 4 |
| Site | DC1 225-230 | |
| Severity | Minor | |
| Time triggered | Fri Jun 28 14:43:27 UTC 2019 | |
| Job | storagegrid | |
| Service | ldr | |

DC1-S2-227

| | |
|-----------------------|------------------------------|
| Node | DC1-S2-227 |
| Site | DC1 225-230 |
| Severity | Minor |
| Time triggered | Fri Jun 28 14:43:27 UTC 2019 |
| Job | storagegrid |
| Service | ldr |

Sent from: DC1-ADM1-225

5

| Llamada | Descripción |
|---------|---|
| 1 | El nombre de la alerta, seguido del número de instancias activas de esta alerta. |
| 2 | La descripción de la alerta. |
| 3 | Todas las acciones recomendadas para la alerta. |
| 4 | Detalles sobre cada instancia activa de la alerta, incluido el nodo y el sitio afectados, la gravedad de la alerta, la hora UTC en la que se activó la regla de alerta y el nombre del trabajo y el servicio afectados. |
| 5 | El nombre de host del nodo de administrador que envió la notificación. |

Cómo se agrupan las alertas

Para evitar que se envíe un número excesivo de notificaciones por correo electrónico cuando se activan alertas, StorageGRID intenta agrupar varias alertas en la misma notificación.

Consulte la tabla siguiente para ver ejemplos de cómo StorageGRID agrupa varias alertas en notificaciones por correo electrónico.

| Comportamiento | Ejemplo |
|---|--|
| Cada notificación de alerta sólo se aplica a las alertas con el mismo nombre. Si al mismo tiempo se activan dos alertas con nombres diferentes, se envían dos notificaciones por correo electrónico. | <ul style="list-style-type: none"> La alerta A se activa en dos nodos al mismo tiempo. Sólo se envía una notificación. La alerta A se activa en el nodo 1 y la alerta B se activa en el nodo 2 al mismo tiempo. Se envían dos notificaciones: Una para cada alerta. |
| Para una alerta específica de un nodo específico, si los umbrales se alcanzan para más de una gravedad, solo se envía una notificación para la alerta más grave. | <ul style="list-style-type: none"> Se activa la alerta A y se alcanzan los umbrales menores, principales y críticos. Se envía una notificación para la alerta crucial. |
| La primera vez que se activa una alerta, StorageGRID espera 2 minutos antes de enviar una notificación. Si se activan otras alertas con el mismo nombre durante ese tiempo, StorageGRID agrupa todas las alertas en la notificación inicial. | <ol style="list-style-type: none"> La alerta A se activa en el nodo 1 a las 08:00. No se envía ninguna notificación. La alerta A se activa en el nodo 2 a las 08:01. No se envía ninguna notificación. A las 08:02, se envía una notificación para informar de ambas instancias de la alerta. |
| Si se activa otra alerta con el mismo nombre, StorageGRID espera 10 minutos antes de enviar una nueva notificación. La nueva notificación informa de todas las alertas activas (alertas actuales que no se han silenciado), aunque se hayan notificado previamente. | <ol style="list-style-type: none"> La alerta A se activa en el nodo 1 a las 08:00. Se envía una notificación a las 08:02. La alerta A se activa en el nodo 2 a las 08:05. Una segunda notificación se envía a las 08:15 (10 minutos más tarde). Se informa de ambos nodos. |
| Si existen varias alertas actuales con el mismo nombre y se resuelve una de esas alertas, no se envía una nueva notificación si la alerta se vuelve a producir en el nodo para el que se solucionó la alerta. | <ol style="list-style-type: none"> Se activa la alerta A para el nodo 1. Se envía una notificación. Se activa la alerta A para el nodo 2. Se envía una segunda notificación. La alerta A se ha resuelto para el nodo 2, pero sigue estando activa para el nodo 1. La alerta A se vuelve a activar para el nodo 2. No se envía ninguna notificación nueva porque la alerta sigue activa para el nodo 1. |
| StorageGRID continúa enviando notificaciones por correo electrónico una vez cada 7 días hasta que se resuelven todas las instancias de la alerta o se silencia la regla de alerta. | <ol style="list-style-type: none"> La alerta A se activa para el nodo 1 el 8 de marzo. Se envía una notificación. La alerta A no se resuelve o se silencia. Las notificaciones adicionales se envían el 15 de marzo, el 22 de marzo, el 29 de marzo, etc. |

Solucionar problemas de notificaciones de correo electrónico de alertas

Si se activa la alerta **error de notificación por correo electrónico** o no puede recibir la notificación por correo electrónico de alerta de prueba, siga estos pasos para resolver el problema.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Usted tiene el "[Gestionar alertas o permisos de acceso raíz](#)".

Pasos

1. Compruebe la configuración.
 - a. Seleccione **Alertas > Configuración de correo electrónico**.
 - b. Compruebe que la configuración del servidor de correo electrónico (SMTP) es correcta.
 - c. Compruebe que ha especificado direcciones de correo electrónico válidas para los destinatarios.
2. Compruebe el filtro de spam y asegúrese de que el correo electrónico no se ha enviado a una carpeta basura.
3. Pídale al administrador de correo electrónico que confirme que los correos electrónicos de la dirección del remitente no están siendo bloqueados.
4. Recoja un archivo de registro del nodo de administración y póngase en contacto con el soporte técnico.

El soporte técnico puede utilizar la información de los registros para determinar el problema. Por ejemplo, el archivo prometheus.log podría mostrar un error al conectarse al servidor especificado.

Consulte "[Recopilar archivos de registro y datos del sistema](#)".

Silenciar notificaciones de alerta

Opcionalmente, puede configurar silencios para suprimir temporalmente las notificaciones de alerta.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Usted tiene el "[Gestionar alertas o permisos de acceso raíz](#)".

Acerca de esta tarea

Puede silenciar las reglas de alerta en todo el grid, un sitio único o un nodo individual, así como en una o más gravedades. Cada silencio suprime todas las notificaciones para una sola regla de alerta o para todas las reglas de alerta.

Si ha habilitado el agente SNMP, las silencias también suprimen las capturas SNMP e informan.



Tenga cuidado al decidir silenciar una regla de alerta. Si silencia una alerta, es posible que no detecte un problema subyacente hasta que impida que se complete una operación crítica.

Pasos

1. Seleccione **Alertas > Silencios**.

Aparece la página silencios.

Silences

You can configure silences to temporarily suppress alert notifications. Each silence suppresses the notifications for an alert rule at one or more severities. You can suppress an alert rule on the entire grid, a single site, or a single node.

| Alert Rule | Description | Severity | Time Remaining | Nodes |
|-------------------|-------------|----------|----------------|-------|
| No results found. | | | | |

2. Seleccione **Crear**.

Aparece el cuadro de diálogo Crear silencio.

Create Silence

Alert Rule:

Description (optional):

Duration: Minutes ▾

Severity: Minor only Minor, major Minor, major, critical

Nodes:

- StorageGRID Deployment
 - Data Center 1
 - DC1-ADM1
 - DC1-G1
 - DC1-S1
 - DC1-S2
 - DC1-S3

Cancel Save

3. Seleccione o introduzca la siguiente información:

| Campo | Descripción |
|-----------------|---|
| Regla de alerta | Nombre de la regla de alerta que se desea silenciar. Puede seleccionar cualquier regla de alerta predeterminada o personalizada, incluso si la regla de alerta está desactivada. Nota: Seleccione todas las reglas si desea silenciar todas las reglas de alerta utilizando los criterios especificados en este cuadro de diálogo. |

| Campo | Descripción |
|-------------|---|
| Descripción | Opcionalmente, una descripción del silencio. Por ejemplo, describa el propósito de este silencio. |
| Duración | <p>Cuánto tiempo desea que este silencio permanezca en vigor, en minutos, horas o días. Un silencio puede estar en vigor de 5 minutos a 1,825 días (5 años).</p> <p>Nota: no debe silenciar una regla de alerta por un período prolongado de tiempo. Si se silencia una regla de alerta, es posible que no detecte un problema subyacente hasta que impida que se complete una operación crítica. Sin embargo, es posible que tenga que utilizar un silencio extendido si una alerta se activa mediante una configuración intencional específica, como puede ser el caso de las alertas * Services Appliance LINK down* y las alertas Storage Appliance LINK down.</p> |
| Gravedad | Qué gravedad o gravedad de alerta se deben silenciar. Si la alerta se activa en una de las gravedades seleccionadas, no se enviarán notificaciones. |
| Nodos | <p>A qué nodo o nodos desea que se aplique este silencio. Puede suprimir una regla de alerta o todas las reglas de toda la cuadrícula, un único sitio o un solo nodo. Si selecciona toda la cuadrícula, el silencio se aplica a todos los sitios y a todos los nodos. Si selecciona un sitio, el silencio sólo se aplica a los nodos de ese sitio.</p> <p>Nota: No puedes seleccionar más de un nodo o más de un sitio para cada silencio. Debe crear silencios adicionales si desea suprimir la misma regla de alerta en más de un nodo o más de un sitio a la vez.</p> |

4. Seleccione **Guardar**.

5. Si desea modificar o finalizar un silencio antes de que caduque, puede editarlo o eliminarlo.

| Opción | Descripción |
|-------------------|--|
| Edite un silencio | <ol style="list-style-type: none"> Seleccione Alertas > Silencios. En la tabla, seleccione el botón de opción para el silencio que desea editar. Seleccione Editar. Cambie la descripción, la cantidad de tiempo restante, las gravedades seleccionadas o el nodo afectado. Seleccione Guardar. |

| Opción | Descripción |
|---------------------|---|
| Elimine un silencio | <p>a. Seleccione Alertas > Silencios.</p> <p>b. En la tabla, seleccione el botón de radio para el silencio que desea eliminar.</p> <p>c. Seleccione Quitar.</p> <p>d. Seleccione Aceptar para confirmar que desea eliminar este silencio.</p> <p>Nota: Las notificaciones se enviarán ahora cuando se active esta alerta (a menos que se suprima por otro silencio). Si esta alerta se encuentra activada actualmente, es posible que transcurran unos minutos hasta que se envíen notificaciones de correo electrónico o SNMP, y que la página Alertas deba actualizar.</p> |

Información relacionada

["Configure el agente SNMP"](#)

Referencia de alertas

Esta referencia muestra las alertas por defecto que aparecen en Grid Manager. Las acciones recomendadas están en el mensaje de alerta que recibe.

Según sea necesario, puede crear reglas de alerta personalizadas que se ajusten a su enfoque de administración del sistema.

Algunas de las alertas por defecto utilizan ["Métricas de Prometheus"](#).

Alertas del dispositivo

| Nombre de alerta | Descripción |
|--|--|
| La batería del dispositivo ha caducado | La batería de la controladora de almacenamiento del dispositivo caducó. |
| Error de la batería del aparato | Se produjo un error en la batería de la controladora de almacenamiento del dispositivo. |
| La batería del aparato no tiene suficiente capacidad adquirida | La batería de la controladora de almacenamiento del aparato no tiene suficiente capacidad adquirida. |
| La batería del aparato está a punto de agotarse | La batería del controlador de almacenamiento del dispositivo está casi agotada. |
| Se quitó la batería del aparato | Falta la batería del controlador de almacenamiento del aparato. |
| La batería del aparato está demasiado caliente | La batería del controlador de almacenamiento del aparato se sobrecalienta. |

| Nombre de alerta | Descripción |
|---|--|
| Error de comunicación de la BMC del dispositivo | Se ha perdido la comunicación con el controlador de administración de la placa base (BMC). |
| Se ha detectado un fallo en el dispositivo de arranque del dispositivo | Se ha detectado un problema con el dispositivo de arranque en el dispositivo. |
| Error del dispositivo de backup de la caché del dispositivo | Se produjo un error en un dispositivo de backup de caché persistente. |
| La capacidad del dispositivo de backup de la caché del dispositivo es insuficiente | La capacidad del dispositivo de copia de seguridad de la caché es insuficiente. |
| Dispositivo de backup de la caché de dispositivo con protección contra escritura | Un dispositivo de backup de caché está protegido contra escritura. |
| El tamaño de la memoria caché del dispositivo no coincide | Las dos controladoras del dispositivo tienen distintos tamaños de caché. |
| Fallo de la batería CMOS del aparato | Se ha detectado un problema con la batería CMOS del aparato. |
| Temperatura del chasis de la controladora de computación del dispositivo demasiado alta | La temperatura de la controladora de computación en un dispositivo StorageGRID superó un umbral nominal. |
| Temperatura de CPU del controlador de computación del dispositivo demasiado alta | La temperatura de la CPU en la controladora de computación en un dispositivo StorageGRID superó un umbral nominal. |
| La controladora de computación del dispositivo requiere atención | Se detectó un error de hardware en la controladora de computación de un dispositivo StorageGRID. |
| El suministro De alimentación De la controladora de computación del dispositivo A tiene un problema | El suministro de alimentación A en la controladora de computación tiene un problema. |
| El suministro de alimentación B de la controladora de computación del dispositivo tiene un problema | El suministro de alimentación B en la controladora de computación tiene un problema. |
| El servicio de supervisión del hardware de computación del dispositivo está estancado | El servicio que supervisa el estado del hardware de almacenamiento se ha detenido. |

| Nombre de alerta | Descripción |
|---|---|
| La unidad DAS del dispositivo supera el límite para los datos escritos al día | Cada día se escribe una cantidad excesiva de datos en una unidad, lo que puede anular su garantía. |
| Fallo de la unidad DAS del dispositivo detectado | Se detectó un problema con una unidad de almacenamiento de conexión directa (DAS) en el dispositivo. |
| La unidad DAS del dispositivo está en la ranura o nodo incorrecto | Una unidad de almacenamiento de conexión directa (DAS) está en la ranura o nodo incorrecto |
| Luz localizadora de la unidad DAS del dispositivo encendida | La luz localizadora de unidades para una o varias unidades de almacenamiento de conexión directa (DAS) en un nodo de almacenamiento de dispositivos está encendida. |
| Reconstrucción de la unidad DAS del dispositivo | Se está recompilando una unidad de almacenamiento de conexión directa (DAS). Esto se espera si se reemplazó o se retiró/reinsertó recientemente. |
| Se ha detectado un fallo en el ventilador del dispositivo | Se ha detectado un problema con una unidad de ventilador en el aparato. |
| Se ha detectado un error de Fibre Channel del dispositivo | Se detectó un problema de enlace de Fibre Channel entre la controladora de almacenamiento del dispositivo y la controladora de computación |
| Error en el puerto HBA del Fibre Channel del dispositivo | Un puerto HBA Fibre Channel está fallando o ya falló. |
| Las unidades de memoria caché flash del dispositivo no son óptimas | Las unidades que se usan para la caché SSD no están en estado óptimo. |
| Se quitó la interconexión del dispositivo/el contenedor de batería | Falta el contenedor de interconexión/batería. |
| Falta el puerto LACP del dispositivo | Un puerto de un dispositivo StorageGRID no participa en el enlace LACP. |
| Fallo de NIC del dispositivo detectado | Se ha detectado un problema con una tarjeta de interfaz de red (NIC) en el dispositivo. |
| Se ha degradado el suministro de alimentación general del dispositivo | La potencia de un dispositivo StorageGRID se ha desviado de la tensión de funcionamiento recomendada. |
| Se requiere actualización del software del sistema operativo SANtricity del dispositivo | La versión del software SANtricity es inferior al mínimo recomendado para esta versión de StorageGRID. |

| Nombre de alerta | Descripción |
|---|---|
| Advertencia crítica del SSD del dispositivo | El SSD de un dispositivo notifica una advertencia crítica. |
| Fallo de la controladora A del almacenamiento del dispositivo | Se produjo un error en la controladora De almacenamiento A de un dispositivo StorageGRID. |
| Fallo del controlador B de almacenamiento del dispositivo | Error de la controladora de almacenamiento B en un dispositivo StorageGRID. |
| Fallo de la unidad de la controladora de almacenamiento del dispositivo | Una o varias unidades de un dispositivo StorageGRID presenta errores o no están en estado óptimo. |
| Problema de hardware de la controladora de almacenamiento del dispositivo | El software SANtricity informa "necesita atención" para un componente de un dispositivo StorageGRID. |
| Fallo en la alimentación de la controladora de almacenamiento del dispositivo | La fuente De alimentación A de un dispositivo StorageGRID se ha desviado de la tensión de funcionamiento recomendada. |
| Fallo en la fuente de alimentación B de la controladora de almacenamiento del dispositivo | La fuente de alimentación B de un dispositivo StorageGRID se ha desviado de la tensión de funcionamiento recomendada. |
| El servicio de supervisión del hardware de almacenamiento del dispositivo está estancado | El servicio que supervisa el estado del hardware de almacenamiento se ha detenido. |
| Las bandejas de almacenamiento del dispositivo degradadas | El estado de uno de los componentes de la bandeja de almacenamiento de un dispositivo de almacenamiento es degradado. |
| Se ha superado la temperatura del aparato | Se ha excedido la temperatura nominal o máxima del controlador de almacenamiento del aparato. |
| Se ha eliminado el sensor de temperatura del aparato | Se ha quitado un sensor de temperatura. |
| Error de inicio seguro de UEFI del dispositivo | Un dispositivo no se ha arrancado de forma segura. |
| La actividad de I/o del disco es muy lenta | Es posible que las operaciones de I/O de disco muy lentas estén afectando al rendimiento del grid. |
| Fallo del ventilador del dispositivo de almacenamiento detectado | Se detectó un problema con una unidad de ventilador en el controlador de almacenamiento para un dispositivo. |

| Nombre de alerta | Descripción |
|---|---|
| Conectividad del almacenamiento del dispositivo de almacenamiento degradada | Hay un problema con una o varias conexiones entre la controladora de computación y la controladora de almacenamiento. |
| Dispositivo de almacenamiento inaccesible | No se puede acceder a un dispositivo de almacenamiento. |

Alertas de auditoría y syslog

| Nombre de alerta | Descripción |
|---|--|
| Los registros de auditoría se están agregando a la cola de la memoria | El nodo no puede enviar registros al servidor syslog local y la cola en memoria se está llenando. |
| Error de reenvío del servidor de syslog externo | El nodo no puede reenviar registros al servidor de syslog externo. |
| Cola de auditoría grande | La cola de disco para mensajes de auditoría está llena. Si no se soluciona esta condición, las operaciones de S3 podrían fallar. |
| Los registros se están agregando a la cola del disco | El nodo no puede reenviar registros al servidor de syslog externo y la cola en disco se está llenando. |

Alertas de bloques

| Nombre de alerta | Descripción |
|--|---|
| El bloque de FabricPool tiene una configuración de coherencia de bloques no compatible | Un bucket de FabricPool utiliza el nivel de coherencia disponible o de sitio sólido, que no se admite. |
| El bloque de FabricPool tiene una configuración de control de versiones no compatible | Un bucket de FabricPool tiene activado el control de versiones o el bloqueo de objetos S3, que no están soportados. |

Alertas de Cassandra

| Nombre de alerta | Descripción |
|--|---|
| Error del compactador automático de Cassandra | El compactador automático Cassandra ha experimentado un error. |
| Las métricas del compactador automático de Cassandra no están actualizadas | Las métricas que describen al compactador automático Cassandra no están actualizadas. |

| Nombre de alerta | Descripción |
|---|--|
| Error de comunicación de Cassandra | Los nodos que ejecutan el servicio Cassandra tienen problemas para comunicarse entre sí. |
| Compacciones de Cassandra sobrecargadas | El proceso de compactación de Cassandra está sobrecargado. |
| Error de escritura de sobretamaño de Cassandra | Un proceso StorageGRID interno envió una solicitud de escritura a Cassandra que era demasiado grande. |
| Las métricas de reparación de Cassandra están desfasadas | Las métricas que describen los trabajos de reparación de Cassandra están desactualizadas. |
| El progreso de reparación de Cassandra es lento | El progreso de las reparaciones de la base de datos de Cassandra es lento. |
| El servicio de reparación de Cassandra no está disponible | El servicio de reparación de Cassandra no está disponible. |
| Tablas dañadas en Cassandra | Cassandra detectó daños en la tabla. Cassandra se reinicia automáticamente si detecta daños en la tabla. |

Alertas de Cloud Storage Pool

| Nombre de alerta | Descripción |
|--|---|
| Error de conectividad del pool de almacenamiento en cloud | La comprobación del estado de Cloud Storage Pools detectó uno o más errores nuevos. |
| IAM Roles Anywhere Vencimiento de certificación de entidad final | El certificado de entidad final de IAM Roles Anywhere está a punto de caducar. |

Alertas de replicación entre grid

| Nombre de alerta | Descripción |
|---|---|
| Error permanente de replicación entre grid | Se ha producido un error de replicación entre redes que requiere la intervención del usuario para resolverlo. |
| Recursos de replicación entre grid no disponibles | Las solicitudes de replicación entre grid están pendientes porque un recurso no está disponible. |

Alertas DHCP

| Nombre de alerta | Descripción |
|-------------------------------------|---|
| El arrendamiento DHCP ha caducado | El arrendamiento DHCP de una interfaz de red caducó. |
| El arrendamiento DHCP caduca pronto | El arrendamiento DHCP de una interfaz de red caduca pronto. |
| Servidor DHCP no disponible | El servidor DHCP no está disponible. |

Alertas de depuración y seguimiento

| Nombre de alerta | Descripción |
|--|--|
| Depuración del impacto en el rendimiento | Cuando el modo de depuración está activado, el rendimiento del sistema puede verse afectado negativamente. |
| Configuración de seguimiento activada | Cuando la configuración de seguimiento está habilitada, el rendimiento del sistema puede verse afectado negativamente. |

Alertas por correo electrónico y AutoSupport

| Nombre de alerta | Descripción |
|---|--|
| No se pudo enviar el mensaje de AutoSupport | No se puede enviar el mensaje de AutoSupport más reciente. |
| Error de resolución del nombre de dominio | El nodo StorageGRID no ha podido resolver los nombres de dominio. |
| Error en la notificación por correo electrónico | No se pudo enviar la notificación por correo electrónico para una alerta. |
| No se encontró el depósito de destino del archivo de registro | Falta el depósito de destino de archivo de registros, lo que impide que los registros se archiven en el depósito de destino. |
| SNMP informa a los errores | Errores al enviar notificaciones SNMP informan a un destino de captura. |
| Acceso externo SSH habilitado | El acceso externo SSH ha estado habilitado durante más de 24 horas. |
| Se ha detectado el inicio de sesión de la consola o SSH | En las últimas 24 horas, un usuario ha iniciado sesión con Web Console o SSH. |

Alertas de código de borrado (EC)

| Nombre de alerta | Descripción |
|---|--|
| Fallo de reequilibrio de EC | El procedimiento de reequilibrio de EC ha fallado o se ha detenido. |
| Fallo de reparación de EC | Se ha producido un error en un trabajo de reparación de los datos de EC o se ha detenido. |
| Reparación EC bloqueada | Se ha detenido un trabajo de reparación para los datos de EC. |
| Error de verificación de fragmentos con código de borrado | Ya no es posible verificar los fragmentos de código de borrado. Es posible que los fragmentos corruptos no se reparen. |

Caducidad de las alertas de certificados

| Nombre de alerta | Descripción |
|---|--|
| Caducidad del certificado de CA de proxy de administración | Uno o varios certificados del paquete de CA de servidor proxy de administración están a punto de caducar. |
| Vencimiento del certificado de cliente | Uno o más certificados de cliente están a punto de caducar. |
| Vencimiento del certificado de servidor global para S3 | El certificado de servidor global para S3 está a punto de caducar. |
| Caducidad del certificado de extremo de equilibrador de carga | Uno o más certificados de punto final de equilibrio de carga están a punto de expirar. |
| Caducidad del certificado de servidor para la interfaz de gestión | El certificado de servidor utilizado para la interfaz de gestión está a punto de expirar. |
| Vencimiento del certificado de CA de syslog externo | El certificado de la entidad de certificación (CA) utilizado para firmar el certificado de servidor de syslog externo está a punto de expirar. |
| Vencimiento del certificado de cliente de syslog externo | El certificado de cliente para un servidor de syslog externo está a punto de expirar. |
| Vencimiento del certificado de servidor de syslog externo | El certificado de servidor presentado por el servidor de syslog externo está a punto de expirar. |

Alertas de red de grid

| Nombre de alerta | Descripción |
|------------------------------------|--|
| Discrepancia de MTU de red de grid | La configuración de MTU de la interfaz de red de grid (eth0) difiere considerablemente entre los nodos del grid. |

Alertas de federación de grid

| Nombre de alerta | Descripción |
|---|--|
| Caducidad del certificado de federación de grid | Uno o varios certificados de federación de grid están a punto de caducar. |
| Error de conexión de federación de grid | La conexión de federación de grid entre el grid local y el remoto no funciona. |

Alertas de uso elevado o alta latencia

| Nombre de alerta | Descripción |
|---|--|
| Uso de montón Java alto | Se está utilizando un alto porcentaje de espacio de pila Java. |
| Alta latencia para consultas de metadatos | El tiempo medio para las consultas de metadatos de Cassandra es demasiado largo. |

Alertas de federación de identidades

| Nombre de alerta | Descripción |
|---|---|
| Fallo de sincronización de la federación de identidades | No se pueden sincronizar los grupos federados y los usuarios del origen de identidades. |
| Error de sincronización de la federación de identidades para un inquilino | No se pueden sincronizar los grupos federados y los usuarios del origen de identidades configurado por un arrendatario. |

Alertas de gestión de la vida útil de la información (ILM)

| Nombre de alerta | Descripción |
|---------------------------------------|---|
| Se puede lograr una colocación de ILM | No se puede obtener una instrucción de colocación en una regla de ILM para ciertos objetos. |
| Tasa baja de análisis de ILM | La tasa de análisis de ILM se establece en menos de 100 objetos por segundo. |

Alertas del servidor de gestión de claves (KMS)

| Nombre de alerta | Descripción |
|--|---|
| Vencimiento DEL certificado de CA DE KMS | El certificado de la entidad de certificación (CA) utilizado para firmar el certificado de servidor de gestión de claves (KMS) está a punto de expirar. |

| Nombre de alerta | Descripción |
|---|---|
| Vencimiento del certificado de cliente DE KMS | El certificado de cliente para un servidor de gestión de claves está a punto de caducar |
| No se ha podido cargar la configuración DE KMS | La configuración del servidor de gestión de claves existe, pero no pudo cargar. |
| Error de conectividad DE KMS | Un nodo de dispositivo no pudo conectarse con el servidor de gestión de claves para su sitio. |
| No se ha encontrado el nombre de la clave de cifrado DE KMS | El servidor de gestión de claves configurado no tiene una clave de cifrado que coincida con el nombre proporcionado. |
| Error en la rotación de la clave de cifrado DE KMS | Todos los volúmenes del dispositivo se descifraron correctamente, pero uno o más volúmenes no pudieron rotar a la última clave. |
| KMS no está configurado | No existe ningún servidor de gestión de claves para este sitio. |
| LA clave KMS no pudo descifrar el volumen de un dispositivo | Uno o más volúmenes de un dispositivo con el cifrado de nodos activado no se pudieron descifrar con la clave KMS actual. |
| Vencimiento del certificado DEL servidor DE KMS | El certificado de servidor que utiliza el servidor de gestión de claves (KMS) está a punto de expirar. |
| Fallo de conectividad del servidor KM | Un nodo de dispositivo no ha podido conectarse a uno o más servidores del clúster de servidores de gestión de claves de su sitio. |

Alertas del balanceador de carga

| Nombre de alerta | Descripción |
|---|---|
| Conexiones elevadas del equilibrador de carga de solicitud cero | Un porcentaje elevado de conexiones para los puntos finales del equilibrador de carga desconectados sin realizar solicitudes. |

Alertas de desplazamiento de reloj local

| Nombre de alerta | Descripción |
|-------------------------------------|--|
| Reloj local de gran desfase horario | El ajuste entre el reloj local y la hora del protocolo de hora de red (NTP) es demasiado grande. |

Alertas de poca memoria o poco espacio

| Nombre de alerta | Descripción |
|--|---|
| Capacidad de disco de registro de auditoría baja | El espacio disponible para los registros de auditoría es bajo. Si no se soluciona esta condición, las operaciones de S3 podrían fallar. |
| Memoria del nodo baja disponible | La cantidad de RAM disponible en un nodo es baja. |
| Poco espacio libre para la piscina de almacenamiento | El espacio disponible para almacenar datos de objetos en el nodo de almacenamiento es bajo. |
| Memoria del nodo instalada baja | La cantidad de memoria instalada en un nodo es baja. |
| Almacenamiento de metadatos bajo | El espacio disponible para almacenar metadatos de objetos es bajo. |
| Capacidad de disco de métrica baja | El espacio disponible para la base de datos de métricas es bajo. |
| Almacenamiento de objetos bajo | El espacio disponible para almacenar datos de objeto es bajo. |
| Anulación de Marca de agua de sólo lectura baja | La anulación de la marca de agua de solo lectura del volumen de almacenamiento es inferior a la marca de agua optimizada mínima para un nodo de almacenamiento. |
| Baja capacidad de disco raíz | El espacio disponible en el disco raíz es bajo. |
| Baja capacidad de datos del sistema | El espacio disponible para /var/local es bajo. Si no se soluciona esta condición, las operaciones de S3 podrían fallar. |
| Bajo espacio libre en el directorio tmp | El espacio disponible en el directorio /tmp es bajo. |

Alertas de red de nodo o nodo

| Nombre de alerta | Descripción |
|---|--|
| No se alcanzó el quórum del ADC | El nodo de almacenamiento con servicio ADC está fuera de línea. Las operaciones de expansión y desmantelamiento están bloqueadas hasta que se restablezca el quórum del ADC. |
| Uso de recepción de red de administración | El uso de recepción en la red de administración es alto. |
| Uso de transmisión de red de administración | El uso de transmisión en la red de administración es alto. |
| Fallo de configuración del firewall | Fallo al aplicar la configuración del firewall. |

| Nombre de alerta | Descripción |
|---|---|
| Extremos de la interfaz de gestión en el modo degradado | Todos los extremos de la interfaz de gestión han vuelto a los puertos predeterminados durante demasiado tiempo. |
| Error de conectividad de red de los nodos | Se han producido errores al transferir datos entre nodos. |
| Error de trama de recepción de red del nodo | Un alto porcentaje de las tramas de red recibidas por un nodo tiene errores. |
| El nodo no está sincronizado con el servidor NTP | El nodo no está sincronizado con el servidor de protocolo de tiempo de red (NTP). |
| El nodo no está bloqueado con el servidor NTP | El nodo no está bloqueado por un servidor de protocolo de tiempo de red (NTP). |
| Red de nodos que no es del dispositivo inactiva | Uno o más dispositivos de red están inactivos o desconectados. |
| Enlace del dispositivo de servicios inactivo en Admin Network | La interfaz del dispositivo a la red de administración (eth1) está inactiva o desconectada. |
| El dispositivo de servicios está desconectado en el puerto de red de administración 1 | El puerto de red de administración 1 del dispositivo está inactivo o desconectado. |
| Enlace del dispositivo de servicios inactivo en la red cliente | La interfaz del dispositivo a la red cliente (eth2) está inactiva o desconectada. |
| Enlace del dispositivo de servicios desactivado en el puerto de red 1 | El puerto de red 1 del dispositivo está inactivo o desconectado. |
| Enlace del dispositivo de servicios desactivado en el puerto de red 2 | El puerto de red 2 del dispositivo está inactivo o desconectado. |
| Enlace del dispositivo de servicios desactivado en el puerto de red 3 | El puerto de red 3 del dispositivo está inactivo o desconectado. |
| Enlace del dispositivo de servicios desactivado en el puerto de red 4 | El puerto de red 4 del dispositivo está inactivo o desconectado. |
| Enlace inactivo del dispositivo de almacenamiento en la red de administración | La interfaz del dispositivo a la red de administración (eth1) está inactiva o desconectada. |

| Nombre de alerta | Descripción |
|--|---|
| Enlace inactivo del dispositivo de almacenamiento en el puerto de red de administrador 1 | El puerto de red de administración 1 del dispositivo está inactivo o desconectado. |
| Enlace del dispositivo de almacenamiento inactivo en la red cliente | La interfaz del dispositivo a la red cliente (eth2) está inactiva o desconectada. |
| Enlace inactivo del dispositivo de almacenamiento en el puerto de red 1 | El puerto de red 1 del dispositivo está inactivo o desconectado. |
| Enlace inactivo del dispositivo de almacenamiento en el puerto de red 2 | El puerto de red 2 del dispositivo está inactivo o desconectado. |
| Enlace inactivo del dispositivo de almacenamiento en el puerto de red 3 | El puerto de red 3 del dispositivo está inactivo o desconectado. |
| Enlace inactivo del dispositivo de almacenamiento en el puerto de red 4 | El puerto de red 4 del dispositivo está inactivo o desconectado. |
| El nodo de almacenamiento no está en el estado de almacenamiento deseado | El servicio LDR de un nodo de almacenamiento no puede realizar la transición al estado deseado debido a un error interno o a un problema relacionado con el volumen |
| Uso de conexión TCP | El número de conexiones TCP en este nodo se acerca al número máximo que se puede realizar el seguimiento. |
| No es posible comunicarse con el nodo | Uno o varios servicios no responden o no se puede acceder al nodo. |
| Reinicio de nodo inesperado | Un nodo se reinició de forma inesperada en las últimas 24 horas. |

Alertas de objetos

| Nombre de alerta | Descripción |
|--|--|
| Error en la comprobación de la existencia del objeto | Error en el trabajo de comprobación de la existencia del objeto. |
| Comprobación de existencia de objeto bloqueada | El trabajo de comprobación de la existencia del objeto se ha detenido. |

| Nombre de alerta | Descripción |
|---|---|
| Objetos potencialmente perdidos | Uno o más objetos potencialmente perdidos de la red. |
| Objetos huérfanos detectados | Se han detectado objetos huérfanos. |
| S3 PUT tamaño de objeto demasiado grande | Un cliente está intentando realizar una operación PUT Object que supera los S3 límites de tamaño. |
| Se detectó un objeto dañado no identificado | Se encontró un archivo en el almacenamiento de objetos replicado que no se pudo identificar como un objeto replicado. |

Alertas de corrupción de objetos

| Nombre de alerta | Descripción |
|---------------------------------|--|
| Desajuste del tamaño del objeto | Se detectó un tamaño de objeto inesperado durante el procedimiento de verificación de existencia del objeto. |

Alertas de servicios de la plataforma

| Nombre de alerta | Descripción |
|--|---|
| Capacidad de solicitud pendiente de servicios de plataforma baja | El número de solicitudes pendientes de servicios de plataforma se acerca a su capacidad. |
| Servicios de plataforma no disponibles | Hay muy pocos nodos de almacenamiento con el servicio RSM en ejecución o disponibles en un sitio. |

Alertas del volumen de almacenamiento

| Nombre de alerta | Descripción |
|---|---|
| El volumen de almacenamiento necesita atención | Un volumen de almacenamiento se encuentra sin conexión y necesita atención. |
| Se debe restaurar el volumen de almacenamiento | Se recuperó un volumen de almacenamiento y debe restaurarse. |
| Volumen de almacenamiento sin conexión | Un volumen de almacenamiento estuvo sin conexión durante más de 5 minutos. |
| Se intentó volver a montar el volumen de almacenamiento | Un volumen de almacenamiento se encontraba sin conexión y se activó un montaje automático. Esto podría indicar un problema de unidad o errores del sistema de archivos. |

| Nombre de alerta | Descripción |
|--|--|
| La restauración de volumen no pudo iniciar la reparación de datos replicados | No se pudo iniciar automáticamente la reparación de datos replicados en un volumen reparado. |

Alertas de servicios StorageGRID

| Nombre de alerta | Descripción |
|--|--|
| servicio nginx mediante la configuración de copia de seguridad | La configuración del servicio nginx no es válida. Ahora se está utilizando la configuración anterior. |
| servicio nginx-gw que utiliza la configuración de copia de seguridad | La configuración del servicio nginx-gw no es válida. Ahora se está utilizando la configuración anterior. |
| Es necesario reiniciar para deshabilitar FIPS | La política de seguridad no requiere el modo FIPS, pero se utilizan módulos FIPS. |
| Es necesario reiniciar para habilitar FIPS | La política de seguridad requiere el modo FIPS, pero los módulos FIPS no están en uso. |
| Servicio SSH mediante la configuración de copia de seguridad | La configuración del servicio SSH no es válida. Ahora se está utilizando la configuración anterior. |

Alertas de inquilinos

| Nombre de alerta | Descripción |
|--------------------------------|--|
| Uso de cuota de inquilino alto | Se está utilizando un alto porcentaje de espacio de cuota. Esta regla está desactivada de forma predeterminada porque podría provocar demasiadas notificaciones. |

Métricas de Prometheus que se usan habitualmente

Consulte esta lista de métricas de Prometheus más utilizadas para comprender mejor las condiciones en las reglas de alerta predeterminadas o para crear las condiciones para reglas de alerta personalizadas.

Usted también puede [obtener una lista completa de todas las métricas](#).

Para obtener más información sobre la sintaxis de las consultas de Prometheus, consulte "[Consultando a Prometeo](#)".

¿Qué son las métricas de Prometheus?

Las métricas de Prometheus son mediciones de series temporales. El servicio Prometheus en los nodos de administración recopila estas métricas de los servicios en todos los nodos. Las métricas se almacenan en cada nodo de administración hasta que se llena el espacio reservado para los datos de Prometheus. Cuando /var/local/mysql_ibdata/ el volumen alcanza su capacidad, primero se eliminan las métricas más antiguas.

¿Dónde se utilizan las métricas de Prometheus?

Las métricas recopiladas por Prometheus se utilizan en varios lugares de Grid Manager:

- **Página de nodos:** Los gráficos y gráficos de las fichas disponibles en la página Nodes utilizan la herramienta de visualización Grafana para mostrar las métricas de series de tiempo recogidas por Prometheus. Grafana muestra los datos de la serie Time en formatos de gráficos y gráficos, mientras que Prometheus sirve como origen de datos del back-end.



- **Alertas:** Las alertas se activan en niveles de gravedad específicos cuando las condiciones de regla de alerta que utilizan las métricas Prometheus se evalúan como verdaderas.
- **API de gestión de grid:** Puede utilizar métricas Prometheus en reglas de alerta personalizadas o con herramientas de automatización externas para supervisar su sistema StorageGRID. Puede consultar una lista completa de la métrica Prometheus en la API de Grid Management. (En la parte superior de Grid Manager, selecciona el ícono de ayuda y selecciona **Documentación de API > Métricas**). Si bien hay más de mil métricas disponibles, solo se requiere una cantidad relativamente pequeña para supervisar las operaciones de StorageGRID más importantes.



Las métricas que incluyen *private* en sus nombres están destinadas únicamente a uso interno y están sujetas a cambios entre versiones de StorageGRID sin previo aviso.

- La página **Soporte > Herramientas > Diagnóstico** y la página **Soporte > Herramientas > Métricas**: estas páginas, que están destinadas principalmente para ser utilizadas por el soporte técnico, proporcionan varias herramientas y gráficos que utilizan los valores de las métricas de Prometheus.



Algunas funciones y elementos de menú de la página Métricas no son intencionalmente funcionales y están sujetos a cambios.

Lista de las métricas más comunes

La siguiente lista contiene las métricas de Prometheus más utilizadas.



Las métricas que incluyen *private* en sus nombres son solo para uso interno y están sujetas a cambios sin previo aviso entre versiones de StorageGRID.

alertmanager_retifications_failed_total

El número total de notificaciones de alertas con errores.

node_filesystem_avail_bytes

La cantidad de espacio del sistema de archivos disponible para los usuarios que no son raíz en bytes.

Node_Memory_MemAvailable_bytes

Campo de información de memoria MemAvailable_bytes.

node_network_carrier

Valor de transportista de /sys/class/net/*iface*.

node_network_receive_errs_total

Estadística de dispositivo de red receive_errs.

node_network_transmit_errs_total

Estadística de dispositivo de red transmit_errs.

storagegrid_administrativamente_down

El nodo no está conectado a la cuadrícula por un motivo esperado. Por ejemplo, el nodo o los servicios del nodo se han apagado correctamente, el nodo se está reiniciando o se está actualizando el software.

storagegrid_appliance_computación_controladora_hardware_status

El estado del hardware de la controladora de computación en un dispositivo.

storagegrid_appliance_failed_discos

Para la controladora de almacenamiento de un dispositivo, la cantidad de unidades que no son óptimas.

storagegrid_dispositivo_almacenamiento_controladora_hardware_status

El estado general del hardware de la controladora de almacenamiento en un dispositivo.

storagegrid_content_buckets_y_contenedores

La cantidad total de depósitos S3 conocidos por este nodo de almacenamiento.

storagegrid_content_objects

La cantidad total de objetos de datos S3 conocidos por este nodo de almacenamiento. El recuento solo es válido para objetos de datos creados por aplicaciones cliente que interactúan con el sistema a través de S3.

storagegrid_content_objects_perdidos

La cantidad total de objetos que este servicio detecta como faltantes en el sistema StorageGRID. Se deben tomar medidas para determinar la causa de la pérdida y si es posible la recuperación.

["Solucionar problemas de datos de objetos perdidos o faltantes"](#)

storagegrid_http_sessions_incoming_attempted

La cantidad total de sesiones HTTP que se intentaron a un nodo de almacenamiento.

storagegrid_http_sessions_incoming_actualmente_establecido

El número de sesiones HTTP activas (abiertas) en el nodo de almacenamiento.

storagegrid_http_sessions_incoming_failed

El número total de sesiones HTTP que no se pudieron completar correctamente, ya sea debido a una solicitud HTTP mal formada o a un error durante el procesamiento de una operación.

storagegrid_http_sessions_incoming_succ

El número total de sesiones HTTP que se completaron correctamente.

storagegrid_ilm_sudeferrent_background_objects

La cantidad total de objetos de este nodo que espera una evaluación de ILM del análisis.

storagegrid_ilm_sudere_client_evaluación_objetos_por_segundo

La velocidad actual a la que se evalúan los objetos en comparación con la política de ILM en este nodo.

storagegrid_ilm_espera_objetos_cliente

El número total de objetos de este nodo a la espera de una evaluación de ILM de operaciones del cliente (por ejemplo, la ingestión).

storagegrid_ilm_espera_total_objetos

La cantidad total de objetos que esperan la evaluación de ILM.

storagegrid_ilm_scan_objects_por_segundo

La velocidad a la que los objetos que posee este nodo se analizan y se colocan en la cola de ILM.

storagegrid_ilm_scan_period_estimated_minutes

El tiempo estimado para completar un análisis completo de ILM en este nodo.

Nota: una exploración completa no garantiza que ILM se haya aplicado a todos los objetos propiedad de este nodo.

storagegrid_load_equilibrador_endpoint_cert_expiry_time

El tiempo de caducidad del certificado de punto final de equilibrio de carga en segundos desde la época.

storagegrid_metadata_consultas_promedio_latencia_milisegundos

Tiempo medio necesario para ejecutar una consulta en el almacén de metadatos a través de este servicio.

storagegrid_network_received_bytes

Cantidad total de datos recibidos desde la instalación.

storagegrid_network_transmisible_bytes

La cantidad total de datos enviados desde la instalación.

storagegrid_node_cpu_utilization_%

El porcentaje de tiempo de CPU disponible que está utilizando actualmente este servicio. Indica el nivel de actividad del servicio. La cantidad de tiempo de CPU disponible depende del número de CPU del servidor.

storagegrid_ntp_elegida_time_source_offset_milisegundos

Desviación sistemática del tiempo proporcionado por una fuente de tiempo seleccionada. La compensación se introduce cuando el retraso hasta llegar a un origen de hora no es igual al tiempo necesario para que el origen de tiempo llegue al cliente NTP.

storagegrid_ntp_locked

El nodo no está bloqueado en un servidor de protocolo de tiempo de redes (NTP).

storagegrid_s3_data_transfers_bytes_ingested

La cantidad total de datos procesados de clientes S3 a este nodo de almacenamiento desde que se restableció el atributo por última vez.

storagegrid_s3_data_transfers_bytes_retrieved

La cantidad total de datos recuperados por clientes S3 de este nodo de almacenamiento desde que se restableció el atributo por última vez.

storagegrid_s3_operations_failed

El número total de operaciones con errores de S3 (códigos de estado HTTP 4xx y 5xx), excepto las causadas por un error de autorización de S3.

storagegrid_s3_operations_successful

La cantidad total de operaciones de S3 correctas (código de estado HTTP 2xx).

storagegrid_s3_operations_unauthorized

El número total de operaciones con errores de S3 que se producen como resultado de un error de autorización.

storagegrid_servercertificate_management_interface_cert_expiry_days

La cantidad de días antes de que caduque el certificado de la interfaz de gestión.

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_días

El número de días antes de que caduque el certificado API de almacenamiento de objetos.

storagegrid_servicio_cpu_segundos

Cantidad acumulada de tiempo que ha utilizado la CPU desde la instalación.

storagegrid_service_memory_usage_bytes

La cantidad de memoria (RAM) actualmente en uso por este servicio. Este valor es idéntico al mostrado por la utilidad Linux top como RES.

storagegrid_servicio_red_received_bytes

La cantidad total de datos recibidos por este servicio desde la instalación.

storagegrid_servicio_red_transmisión_bytes

La cantidad total de datos enviados por este servicio.

storagegrid_servicio_reinicia

El número total de veces que se ha reiniciado el servicio.

storagegrid_service_runtime_segundos

La cantidad total de tiempo que el servicio se ha estado ejecutando desde la instalación.

storagegrid_servicio_tiempo_activo_segundos

La cantidad total de tiempo que el servicio se ha estado ejecutando desde que se reinició por última vez.

storagegrid_storage_state_current

El estado actual de los servicios de almacenamiento. Los valores de atributo son:

- 10 = sin conexión
- 15 = Mantenimiento
- 20 = solo lectura
- 30 = en línea

storagegrid_storage_status

El estado actual de los servicios de almacenamiento. Los valores de atributo son:

- 0 = sin errores
- 10 = en transición
- 20 = espacio libre insuficiente
- 30 = volumen(s) no disponible
- 40 = error

bytes_datos_utilización_almacenamiento_storagegrid

Una estimación del tamaño total de los datos de objetos replicados y codificados de borrado en el nodo de almacenamiento.

storagegrid_storage_utilization_metadata_allowed_bytes

El espacio total en el volumen 0 de cada nodo de almacenamiento permitido para los metadatos de objetos. Este valor es siempre menor que el espacio real reservado para los metadatos en un nodo, ya que una parte del espacio reservado es necesaria para las operaciones esenciales de las bases de datos (como la compactación y reparación) y las futuras actualizaciones de hardware y software. El espacio permitido para los metadatos de objetos controla la capacidad de objetos general.

storagegrid_almacenamiento_utilización_metadatos_bytes

La cantidad de metadatos de objetos en el volumen de almacenamiento 0, en bytes.

storagegrid_storage_utilization_total_space_bytes

La cantidad total de espacio de almacenamiento asignado a todos los almacenes de objetos.

storagegrid_almacenamiento_utilización_espacio_bytes utilizables

La cantidad total de espacio de almacenamiento de objetos restante. Calculado mediante la adición conjunta de la cantidad de espacio disponible para todos los almacenes de objetos en el nodo de almacenamiento.

storagegrid_inquilino_uso_datos_bytes

El tamaño lógico de todos los objetos para el arrendatario.

storagegrid_tenant_usage_object_count

El número de objetos para el arrendatario.

storagegrid_tenant_usage_quota_bytes

La cantidad máxima de espacio lógico disponible para los objetos del inquilino. Si no se proporciona una métrica de cuota, hay disponible una cantidad ilimitada de espacio.

Obtener una lista de todas las métricas

Para obtener la lista completa de métricas, utilice la API de gestión de grid.

Pasos

1. En la parte superior de Grid Manager, selecciona el icono de ayuda y selecciona **Documentación de API**.
2. Localice las operaciones **Metricmétricas**.
3. Ejecute GET /grid/metric-names la operación.
4. Descargue los resultados.

Referencia de archivos de registro

Referencia de archivos de registro

StorageGRID proporciona registros que se utilizan para capturar eventos, mensajes de diagnóstico y condiciones de error. Es posible que se le solicite recoger archivos de registro y reirlos al soporte técnico para ayudar con la solución de problemas.

Los registros se clasifican de la siguiente manera:

- "["Registros del software StorageGRID"](#)
- "["Registros de implementación y mantenimiento"](#)
- "["Acerca de bycast.log"](#)

 Los detalles proporcionados para cada tipo de registro son solo de referencia. Los registros están destinados a la solución de problemas avanzada del soporte técnico. Las técnicas avanzadas que implican la reconstrucción del historial de problemas mediante los registros de auditoría y los archivos de registro de aplicaciones están más allá del alcance de estas instrucciones.

Acceda a los registros

Para acceder a los registros, puede "[recopilar archivos de registro y datos del sistema](#)" desde uno o más nodos como un único archivo de registro. O bien, puede acceder a archivos de registro individuales para cada nodo de la red de la siguiente manera:

Pasos

1. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
2. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
3. Introduzca el siguiente comando para cambiar a raíz: `su -`
4. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Exportar los registros al servidor de syslog

La exportación de registros al servidor de syslog proporciona estas capacidades:

- Reciba una lista de todas las solicitudes de Grid Manager y Tenant Manager, además de las solicitudes de S3.
- Mejor visibilidad de las solicitudes S3 que devuelven errores, sin el impacto en el rendimiento causado por los métodos de registro de auditorías.
- Acceso a solicitudes de capa HTTP y códigos de error que son fáciles de analizar.
- Mejor visibilidad de las solicitudes que fueron bloqueadas por los clasificadores de tráfico en el equilibrador de carga.

Para exportar los registros, consulte "[Configurar la gestión de registros y el servidor syslog externo](#)".

Categorías de archivos de registro

El archivo de registro de StorageGRID contiene los registros descritos para cada categoría y archivos adicionales que contienen métricas y resultados del comando de depuración.

| Ubicación del archivo | Descripción |
|--------------------------------------|--|
| auditoría | Se generan mensajes de auditoría durante el funcionamiento normal del sistema. |
| registros del sistema operativo base | Información sobre el sistema operativo base, incluidas las versiones de imagen StorageGRID. |
| paquetes | Información sobre la configuración global (bundles). |
| servicio de caché | Registros del servicio de caché (solo en nodos de puerta de enlace). |
| cassandra | Información de la base de datos de Cassandra y registros de reparación de Reaper. |
| ce | Información de VCSs sobre el nodo actual y la información de grupo de EC por ID de perfil. |
| cuadrícula | Registros de cuadrícula generales incluidos debug (bypcast.log) y servermanager logs. |
| grid.json | Archivo de configuración de grid compartido en todos los nodos. Además node.json, es específico del nodo actual. |
| regatroups | Métricas y registros de grupos de alta disponibilidad. |
| instale | Gdu-server e instale los registros. |
| Árbitro lambda | Registros relacionados con la solicitud de proxy de S3 Select. |

| Ubicación del archivo | Descripción |
|-----------------------|---|
| filtrado | Registros del servicio leakd. |
| lumberjack.log | Depurar mensajes relacionados con la colección de registros. |
| Métricas | Registros de servicios para Grafana, Jaeger, exportador de nodos y Prometheus. |
| error | Registro de errores y acceso a Missd. |
| mysql | La configuración de la base de datos MariaDB y los registros relacionados. |
| neta | Registros generados por secuencias de comandos relacionadas con la red y el servicio DynIP. |
| nginx | Archivos y registros de configuración de federación de grid y equilibrador de carga. También incluye los registros de tráfico de Grid Manager y del gestor de inquilinos. |
| nginx-gw | <ul style="list-style-type: none"> • access.log: Grid Manager y el gestor de inquilinos solicitan mensajes de registro. <ul style="list-style-type: none"> ◦ Estos mensajes tienen el prefijo mgmt: cuando se exportan mediante syslog. ◦ El formato de estos mensajes de registro es [\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$request" "\$http_host" "\$http_user_agent" "\$http_referer" • cgr-access.log.gz: Solicitudes de replicación entre cuadrículas entrantes. <ul style="list-style-type: none"> ◦ Estos mensajes tienen el prefijo cgr: cuando se exportan mediante syslog. ◦ El formato de estos mensajes de registro es [\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$upstream_addr" "\$request" "\$http_host" • endpoint-access.log.gz: Solicitudes S3 a puntos finales del balanceador de carga. <ul style="list-style-type: none"> ◦ Estos mensajes tienen el prefijo endpoint: cuando se exportan mediante syslog. ◦ El formato de estos mensajes de registro es [\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$upstream_addr" "\$request" "\$http_host" • nginx-gw-dns-check.log: Relacionado con la nueva alerta de comprobación de DNS. |

| Ubicación del archivo | Descripción |
|--------------------------------------|---|
| ntp | Registros y archivo de configuración NTP. |
| Objetos huérfanos | Registros pertenecientes a objetos huérfanos. |
| so | Archivo de estado de nodo y cuadrícula, incluidos los servicios pid. |
| otros | Los archivos de registro /var/local/log que no se recopilan en otras carpetas. |
| rendim | Facilite información sobre el rendimiento de la I/o de disco, red y CPU |
| prometheus-data | Métrica Prometheus actual, si la colección de registros incluye datos Prometheus. |
| el provisionamiento | Registros relacionados con el proceso de aprovisionamiento de grid. |
| balsa | Registros del clúster Raft utilizados en los servicios de la plataforma. |
| ssh | Registros relacionados con la configuración y el servicio SSH. |
| snmp | Configuración del agente SNMP utilizada para enviar notificaciones SNMP. |
| sockets-datos | Sockets de datos para la depuración de red. |
| system-commands.txt | Resultado de los comandos de contenedor de StorageGRID. Contiene información del sistema, como el uso de redes y discos. |
| paquete de recuperación sincronizada | Relacionado con el mantenimiento de la coherencia del último paquete de recuperación en todos los nodos de administración y nodos de almacenamiento que alojan el servicio ADC. |

Registros del software StorageGRID

Los registros de StorageGRID se pueden usar para solucionar problemas.



Si desea enviar sus registros a un servidor syslog externo o cambiar el destino de la información de auditoría, como bycast.log y nms.log , ver "["Configurar la gestión de registros"](#).

Registros de StorageGRID generales

| Nombre de archivo | Notas | Encontrado en |
|---------------------------|--|-----------------|
| /var/local/log/bycast.log | El archivo principal de solución de problemas de StorageGRID . | Todos los nodos |

| Nombre de archivo | Notas | Encontrado en |
|-------------------------------|--|-----------------|
| /var/local/log/bycast-err.log | Contiene un subconjunto de <code>broadcast.log</code> (mensajes con severidad ERROR y CRÍTICO). Los mensajes CRÍTICOS también se muestran en el sistema. | Todos los nodos |
| /var/local/core/ | Contiene cualquier archivo de volcado principal creado si el programa finaliza de forma anormal. Las causas posibles incluyen fallos de aserción, infracciones o tiempos de espera de subprocessos. Nota: El archivo `/var/local/core/kexec_cmd` generalmente existe en los nodos del dispositivo y no indica un error. | Todos los nodos |

Registros relacionados con el cifrado

| Nombre de archivo | Notas | Encontrado en |
|---|---|--|
| /var/local/log/ssh-config-generation.log | Contiene registros relacionados con la generación de configuraciones SSH y la recarga de servicios SSH. | Todos los nodos |
| /var/local/log/nginx/config-generation.log | Contiene registros relacionados con la generación de configuraciones nginx y la recarga de servicios nginx. | Todos los nodos |
| /var/local/log/nginx-gw/config-generation.log | Contiene registros relacionados con la generación de configuraciones nginx-gw (y la recarga de servicios nginx-gw). | Nodos de administración y puerta de enlace |
| /var/local/log/update-cipher-configurations.log | Contiene registros relacionados con la configuración de políticas TLS y SSH. | Todos los nodos |

Registros de federación de grid

| Nombre de archivo | Notas | Encontrado en |
|--|---|-----------------|
| /var/local/log/update_grid_federation_config.log | Contiene registros relacionados con la generación de configuraciones nginx y nginx-gw para conexiones de federación de red. | Todos los nodos |

Registros de NMS

| Nombre de archivo | Notas | Encontrado en |
|-------------------------------|--|-------------------------|
| /var/local/log/nms.log | <ul style="list-style-type: none"> Captura las notificaciones de Grid Manager y del arrendatario Manager. Captura eventos relacionados con el funcionamiento del servicio NMS. Por ejemplo, notificaciones por correo electrónico y cambios de configuración. Contiene actualizaciones del paquete XML como resultado de los cambios de configuración realizados en el sistema. Contiene mensajes de error relacionados con la reducción del atributo realizada una vez al día. Contiene mensajes de error del servidor Web Java, por ejemplo, errores de generación de páginas y errores de estado HTTP 500. | Nodos de administración |
| /var/local/log/nms.errlog | <p>Contiene mensajes de error relacionados con las actualizaciones de la base de datos de MySQL.</p> <p>Contiene la secuencia error estándar (stderr) de los servicios correspondientes. Hay un archivo de registro por servicio. Estos archivos suelen estar vacíos a menos que haya problemas con el servicio.</p> | Nodos de administración |
| /var/local/log/nms.requestlog | Contiene información acerca de las conexiones salientes de la API de administración a los servicios StorageGRID internos. | Nodos de administración |

Registros de Server Manager

| Nombre de archivo | Notas | Encontrado en |
|---------------------------------------|--|-----------------|
| /var/local/log/servermanager.log | Archivo de registro de la aplicación Server Manager que se ejecuta en el servidor. | Todos los nodos |
| /Var/local/log/GridstatBackend.errlog | Archivo de registro para la aplicación de back-end GUI de Server Manager. | Todos los nodos |

| Nombre de archivo | Notas | Encontrado en |
|--------------------------------|--|-----------------|
| /var/local/log/gridstat.errlog | Archivo de registro para la GUI de Server Manager. | Todos los nodos |

Registros de servicios de StorageGRID

| Nombre de archivo | Notas | Encontrado en |
|---|--|--|
| /var/local/log/acct.errlog | | Nodos de almacenamiento que ejecutan el servicio ADC |
| /var/local/log/adc.errlog | Contiene la secuencia error estándar (stderr) de los servicios correspondientes. Hay un archivo de registro por servicio. Estos archivos suelen estar vacíos a menos que haya problemas con el servicio. | Nodos de almacenamiento que ejecutan el servicio ADC |
| /var/local/log/ams.errlog | | Nodos de administración |
| /var/local/log/cache-svc.log + /var/local/log/cache-svc.errlog | Registros del servicio de caché. | Nodos de puerta de enlace |
| /var/local/log/cassandra/system.log | Información del almacén de metadatos (base de datos Cassandra) que se puede utilizar si se producen problemas al agregar nuevos nodos de almacenamiento o si se bloquea la tarea de reparación nodetool. | Nodos de almacenamiento |
| /var/local/log/cassandra-reaper.log | Información del servicio Cassandra Reaper, que realiza reparaciones de los datos de la base de datos Cassandra. | Nodos de almacenamiento |
| /var/local/log/cassandra-reaper.errlog | Información de error para el servicio Cassandra Reaper. | Nodos de almacenamiento |
| /var/local/log/chunk.errlog | | Nodos de almacenamiento |
| /var/local/log/cmn.errlog | | Nodos de administración |
| /var/local/log/cms.errlog | Este archivo de registro puede estar presente en los sistemas que se han actualizado desde una versión anterior de StorageGRID. Contiene información heredada. | Nodos de almacenamiento |

| Nombre de archivo | Notas | Encontrado en |
|------------------------------------|---|--|
| /var/local/log/dds.errlog | | Nodos de almacenamiento |
| /var/local/log/dmv.errlog | | Nodos de almacenamiento |
| /var/local/log/dynip* | Contiene registros relacionados con el servicio dynip, que supervisa la cuadrícula para cambios IP dinámicos y actualiza la configuración local. | Todos los nodos |
| /var/local/log/grafana.log | El registro asociado al servicio Grafana, que se utiliza para la visualización de métricas en Grid Manager. | Nodos de administración |
| /var/local/log/hagroups.log | El registro asociado a los grupos de alta disponibilidad. | Nodos de administrador y nodos de puerta de enlace |
| /var/local/log/hagroups_events.log | Realiza un seguimiento de los cambios de estado, como la transición de UNA COPIA de SEGURIDAD a UNA COPIA MAESTRA o UN FALLO. | Nodos de administrador y nodos de puerta de enlace |
| /var/local/log/idnt.errlog | | Nodos de almacenamiento que ejecutan el servicio ADC |
| /var/local/log/jaeger.log | El registro asociado al servicio jaeger, que se utiliza para la recopilación de trazas. | Todos los nodos |
| /var/local/log/kstn.errlog | | Nodos de almacenamiento que ejecutan el servicio ADC |
| /var/local/log/lambda* | Contiene registros del servicio S3 Select. Solo algunos nodos Admin y Gateway contienen este registro. Consulte la "S3 Select requisitos y limitaciones para los nodos de administración y puerta de enlace" . | Nodos de administración y puerta de enlace |

| Nombre de archivo | Notas | Encontrado en |
|--|---|---|
| /var/local/log/ldr.errlog | | Nodos de almacenamiento |
| /var/local/log/miscd/*.log | Contiene registros para el servicio MISCD (Information Service Control Daemon, Daemon de control del servicio de información), que proporciona una interfaz para consultar y administrar servicios en otros nodos y para administrar configuraciones medioambientales en el nodo, como consultar el estado de los servicios que se ejecutan en otros nodos. | Todos los nodos |
| /var/local/log/nginx/*.log | Contiene registros para el servicio nginx, que actúa como mecanismo de autenticación y comunicación segura para varios servicios de red (como Prometheus y DynIP) para poder hablar con servicios en otros nodos a través de API HTTPS. | Todos los nodos |
| /var/local/log/nginx-gw/*.log | Contiene registros generales relacionados con el servicio nginx-gw, incluidos los registros de errores y los registros de los puertos de administración restringidos en los nodos de administración. | Nodos de administrador y nodos de puerta de enlace |
| /var/local/log/nginx-gw/cgr-access.log.gz | Contiene registros de acceso relacionados con el tráfico de replicación entre grid. | Los nodos de administración, los nodos de puerta de enlace o ambos, según la configuración de federación de grid. Solo se encuentra en la cuadrícula de destino para la replicación entre grid. |
| /var/local/log/nginx-gw/endpoint-access.log.gz | Contiene registros de acceso para el servicio Load Balancer, que proporciona equilibrio de carga del tráfico S3 de clientes a nodos de almacenamiento. | Nodos de administrador y nodos de puerta de enlace |
| /var/local/log/persistence* | Contiene registros del servicio Persistence, que gestiona los archivos en el disco raíz que deben persistir durante un reinicio. | Todos los nodos |

| Nombre de archivo | Notas | Encontrado en |
|---|---|--|
| /var/local/log/prometheus.log | <p>Para todos los nodos, contiene el registro de servicio del exportador de nodos y el registro del servicio de métricas del exportador de nodos.</p> <p>Para los nodos de administrador, también contiene registros de los servicios Prometheus y Alert Manager.</p> | Todos los nodos |
| /var/local/log/raft.log | Contiene la salida de la biblioteca utilizada por el servicio RSM para el protocolo Raft. | Nodos de almacenamiento con servicio RSM |
| /var/local/log/rms.errlog | Contiene registros para el servicio Servicio de máquina de estado replicado (RSM), que se utiliza para los servicios de plataforma S3. | Nodos de almacenamiento con servicio RSM |
| /var/local/log/ssm.errlog | | Todos los nodos |
| /var/local/log/update-s3vs-domains.log | Contiene registros relacionados con el procesamiento de actualizaciones para la configuración de nombres de dominio alojados virtuales de S3. Consulte las instrucciones para implementar aplicaciones cliente S3. | Nodos de administración y puerta de enlace |
| /var/local/log/update-snmp-firewall.* | Contenga registros relacionados con los puertos de firewall que se gestionan para SNMP. | Todos los nodos |
| /var/local/log/update-sysl.log | Contiene registros relacionados con los cambios que se realizan en la configuración de syslog del sistema. | Todos los nodos |
| /var/local/log/update-traffic-classes.log | Contiene registros relacionados con los cambios en la configuración de los clasificadores de tráfico. | Nodos de administración y puerta de enlace |
| /var/local/log/update-utcn.log | Contiene registros relacionados con el modo de red de cliente no confiable en este nodo. | Todos los nodos |

Información relacionada

- ["Acerca de bycast.log"](#)
- ["USE LA API DE REST DE S3"](#)

Registros de implementación y mantenimiento

Puede utilizar los registros de implementación y de mantenimiento para solucionar problemas.

| Nombre de archivo | Notas | Encontrado en |
|---------------------------------------|--|---------------------------------|
| /var/local/log/install.log | Creado durante la instalación del software. Contiene un registro de los eventos de instalación. | Todos los nodos |
| /var/local/log/expansion-progress.log | Creado durante las operaciones de expansión. Contiene un registro de los eventos de expansión. | Nodos de almacenamiento |
| /var/local/log/pa-move.log | Creado al ejecutar el pa-move.sh script. | Nodo de administrador principal |
| /var/local/log/pa-move-new_pa.log | Creado al ejecutar el pa-move.sh script. | Nodo de administrador principal |
| /var/local/log/pa-move-old_pa.log | Creado al ejecutar el pa-move.sh script. | Nodo de administrador principal |
| /var/local/log/gdu-server.log | Creado por el servicio GDU. Contiene eventos relacionados con los procedimientos de aprovisionamiento y mantenimiento gestionados por el nodo de administración principal. | Nodos de administración |
| /var/local/log/send_admin_hw.log | Creado durante la instalación. Contiene información de depuración relacionada con las comunicaciones de un nodo con el nodo de administración principal. | Todos los nodos |
| /var/local/log/upgrade.log | Creado durante la actualización de software. Contiene un registro de los eventos de actualización de software. | Todos los nodos |

Acerca de bycast.log

El archivo /var/local/log/broadcast.log es el archivo principal de solución de problemas del software StorageGRID. Hay un broadcast.log archivo para cada nodo de cuadrícula. El archivo contiene mensajes específicos de ese nodo de cuadrícula.

El archivo /var/local/log/broadcast-err.log es un subconjunto de broadcast.log . Contiene mensajes DE ERROR grave Y CRÍTICOS.

Opcionalmente, puede cambiar el destino de los registros de auditoría y enviar información de auditoría a un servidor syslog externo. Los registros locales de registros de auditoría continúan generándose y almacenándose cuando se configura un servidor syslog externo. Ver "["Configurar la gestión de registros y el servidor syslog externo"](#)" .

Rotación de archivos para bycast.log

Cuando el bycast.log archivo alcanza los 1 GB, se guarda el archivo existente y se inicia un nuevo archivo de registro.

Se cambia el nombre del archivo guardado bycast.log.1 y el nuevo archivo se denomina bycast.log. Cuando el nuevo bycast.log alcanza los 1 GB, bycast.log.1 se cambia el nombre y se comprime para que se convierta en bycast.log.2.gz, y bycast.log se cambia el nombre bycast.log.1.

El límite de rotación para bycast.log es de 21 archivos. Cuando se crea la versión 22nd del bycast.log archivo, se elimina el archivo más antiguo.

El límite de rotación para bycast-err.log es de siete archivos.



Si se ha comprimido un archivo de registro, no debe descomprimirlo en la misma ubicación en la que se escribió. Descomprimir el archivo en la misma ubicación puede interferir con las secuencias de comandos de rotación del registro.

Opcionalmente, puede cambiar el destino de los registros de auditoría y enviar información de auditoría a un servidor syslog externo. Los registros locales de registros de auditoría continúan generándose y almacenándose cuando se configura un servidor syslog externo. Ver "["Configurar la gestión de registros y el servidor syslog externo"](#)" .

Información relacionada

["Recopilar archivos de registro y datos del sistema"](#)

Mensajes en bycast.log

Los mensajes en bycast.log son escritos por el ADE (Entorno distribuido asíncrono). ADE es el entorno de tiempo de ejecución que utilizan los servicios de cada nodo de grid.

Mensaje ADE de ejemplo:

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685      0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

Los mensajes ADE contienen la siguiente información:

| Segmento de mensaje | Valor en ejemplo |
|--------------------------|------------------|
| ID de nodo | 12455685 |
| ID de proceso DE ADE | 0357819531 |
| Nombre del módulo | SVMR |
| Identificador de mensaje | VEHR |

| Segmento de mensaje | Valor en ejemplo |
|-------------------------------|--|
| Hora del sistema UTC | 2019-05-05T27T17:10:29.784677 (YYYYY-MM-DDTHH:MM:SS.UUUUUUUUUUUU) |
| Nivel de gravedad | ERROR |
| Número de seguimiento interno | 0906 |
| Mensaje | SVMR: El control de estado del volumen 3 ha fallado con el motivo "TOUT" |

Niveles de gravedad del mensaje en bycast.log

Los mensajes `broadcast.log` tienen asignados niveles de gravedad.

Por ejemplo:

- **AVISO** — se ha producido un evento que debería registrarse. La mayoría de los mensajes de registro se encuentran en este nivel.
- **ADVERTENCIA** — se ha producido una condición inesperada.
- **ERROR** — se ha producido Un error importante que afectará a las operaciones.
- **CRÍTICO** — se ha producido una condición anormal que ha detenido el funcionamiento normal. Debe abordar la condición subyacente de inmediato.

Códigos de error en `broadcast.log`

La mayoría de los mensajes de error de `broadcast.log` contienen códigos de error.

La siguiente tabla enumera los códigos no numéricos comunes en `broadcast.log`. El significado exacto de un código no numérico depende del contexto en el que se informa.

| Código de error | Significado |
|-----------------|------------------|
| SUCS | Sin error |
| GERR | Desconocido |
| CANC | Cancelada |
| ABRT | Anulado |
| CONSIGUE | Tiempo de espera |
| INVL | No válido |
| NFND | No encontrado |

| Código de error | Significado |
|-----------------|------------------------|
| VERS | Versión |
| CONF | Configuración |
| ERROR | Con errores |
| ICPL | Incompleto |
| LISTO | Listo |
| SVNU | Servicio no disponible |

La siguiente tabla enumera los códigos de error numéricos en `broadcast.log`.

| Número de error | Código de error | Significado |
|-----------------|-----------------|---|
| 001 | EPERM | Operación no permitida |
| 002 | ENOENT | No existe el archivo o directorio |
| 003 | ESRCH | No hay tal proceso |
| 004 | EINTR | Llamada de sistema interrumpida |
| 005 | EIO | Error de E/S. |
| 006 | ENXIO | No existe el dispositivo o la dirección |
| 007 | E2BIG | Lista de argumentos demasiado larga |
| 008 | ENOEXEC | Error de formato ejecutivo |
| 009 | EBADF | Número de archivo incorrecto |
| 010 | ECHILD | No hay procesos secundarios |
| 011 | EAGAIN | Inténtelo de nuevo |
| 012 | ENOMEM | Memoria insuficiente |
| 013 | EACCES | Permiso denegado |

| Número de error | Código de error | Significado |
|-----------------|-----------------|---|
| 014 | PREDETERMINADO | Dirección incorrecta |
| 015 | ENOTBLK | Dispositivo de bloques requerido |
| 016 | EBUSY | Dispositivo o recurso ocupado |
| 017 | EXIST | El archivo existe |
| 018 | EXDEV | Enlace entre dispositivos |
| 019 | ENDEV | No existe dicho dispositivo |
| 020 | ENOTDIR | No es un directorio |
| 021 | EISDIR | Es un directorio |
| 022 | EINVAL | Argumento no válido |
| 023 | INFORMACIÓN | Desbordamiento de tabla de archivo |
| 024 | ARCHIVO | Demasiados archivos abiertos |
| 025 | RESPONSABILIDAD | No es una máquina de escribir |
| 026 | ETXTBSY | Archivo de texto ocupado |
| 027 | EFBIG | Archivo demasiado grande |
| 028 | ENOSPC | No queda espacio en el dispositivo |
| 029 | ESPIPE | Búsqueda ilegal |
| 030 | EROFS | Sistema de archivos de solo lectura |
| 031 | EMLINK | Demasiados enlaces |
| 032 | LIMPIEZA | Tubo roto |
| 033 | EDOM | Argumento matemático fuera de dominio de func |
| 034 | ENGE | Resultado de matemáticas no representable |

| Número de error | Código de error | Significado |
|-----------------|-----------------|---|
| 035 | EDADLK | Se producirá un interbloqueo de recursos |
| 036 | ENAMETOOLONG | El nombre del archivo es demasiado largo |
| 037 | ENOLCK | No hay bloqueos de grabación disponibles |
| 038 | ENOSYS | Función no implementada |
| 039 | ENOTEMPTY | Directorio no vacío |
| 040 | ELOOP | Se han encontrado demasiados enlaces simbólicos |
| 041 | | |
| 042 | ENOMSG | No hay mensaje del tipo deseado |
| 043 | EIDRM | Se ha eliminado el identificador |
| 044 | ECHRNG | Número de canal fuera de rango |
| 045 | EL2NSYNC | Nivel 2 no sincronizado |
| 046 | EL3HLT | Nivel 3 detenido |
| 047 | EL3RST | Reinicio del nivel 3 |
| 048 | ELNRNG | Número de enlace fuera de rango |
| 049 | EUNATCH | Controlador de protocolo no adjunto |
| 050 | ENOCSI | No hay estructura CSI disponible |
| 051 | EL2HLT | Nivel 2 detenido |
| 052 | EBADE | Intercambio no válido |
| 053 | EBADR | Descriptor de solicitud no válido |
| 054 | EXFULL | Intercambio lleno |
| 055 | ENANO | Sin ánodo |

| Número de error | Código de error | Significado |
|-----------------|-----------------|---|
| 056 | EBADRQC | Código de solicitud no válido |
| 057 | EBADSLT | Ranura no válida |
| 058 | | |
| 059 | EBFONT | Formato de archivo de fuentes incorrecto |
| 060 | ENOSTR | El dispositivo no es un flujo |
| 061 | ENODATA | No hay datos disponibles |
| 062 | ETIME | El temporizador ha caducado |
| 063 | ENOSR | Recursos de fuera de flujo |
| 064 | ENONET | El equipo no está en la red |
| 065 | OPKG | Paquete no instalado |
| 066 | EREMOTE | El objeto es remoto |
| 067 | ENELINK | El enlace se ha cortado |
| 068 | EADV | Error en la Publicidad |
| 069 | ESRMNT | Error de Srmount |
| 070 | ECOMM | Error de comunicación al enviar |
| 071 | EPROTO | Error de protocolo |
| 072 | EMULTIHOP | Intento de multisalto |
| 073 | EDOTDOT | Error específico de RFS |
| 074 | EBADMSG | No es un mensaje de datos |
| 075 | EOVERFLOW | Valor demasiado grande para el tipo de datos definido |
| 076 | ENOTUNIQ | El nombre no es único en la red |

| Número de error | Código de error | Significado |
|-----------------|-----------------|---|
| 077 | EBADFD | Descriptor de archivo en estado incorrecto |
| 078 | EREMCHG | Se cambió la dirección remota |
| 079 | ELIBACC | No se puede acceder a una biblioteca compartida necesaria |
| 080 | ELIBBAD | Acceso a una biblioteca compartida dañada |
| 081 | ELIBSCN | |
| 082 | ELIBMAX | Intentando vincular demasiadas bibliotecas compartidas |
| 083 | ELIBEXEC | No se puede ejecutar una biblioteca compartida directamente |
| 084 | EILSEQ | Secuencia de bytes no válida |
| 085 | ERESTART | Debe reiniciarse la llamada del sistema interrumpida |
| 086 | ESTRPIPE | Error de canalización de flujos |
| 087 | EUSERS | Demasiados usuarios |
| 088 | ENOTSOCK | Funcionamiento del conector hembra en el enchufe no hembra |
| 089 | EDESTADDRREQ | Dirección de destino requerida |
| 090 | EMSGSIZE | Mensaje demasiado largo |
| 091 | EPROTOTOLPE | Protocolo tipo incorrecto para socket |
| 092 | ENOTOPT | Protocolo no disponible |
| 093 | EPROTONOSUPPORT | No se admite el protocolo |
| 094 | ESOCKTNOSUPPORT | Tipo de socket no admitido |
| 095 | OPNOTSUPP | Operación no admitida en el extremo de transporte |
| 096 | EPFNOSTUPPORT | No se admite la familia de protocolos |

| Número de error | Código de error | Significado |
|-----------------|-----------------|---|
| 097 | AFNOSTSUPPORT | Familia de direcciones no compatible con el protocolo |
| 098 | EADDRINUSE | La dirección ya está en uso |
| 099 | EADDRNOTAVAIL | No se puede asignar la dirección solicitada |
| 100 | ENETDOWN | La red está inactiva |
| 101 | NETUNREACH | La red es inaccesible |
| 102 | ENETTRESET | Red se ha perdido la conexión debido al restablecimiento |
| 103 | ECONNABORTED | El software ha provocado que se termine la conexión |
| 104 | ECONNRESET | La conexión se restablece por el interlocutor |
| 105 | ENOBUFS | No hay espacio de búfer disponible |
| 106 | EISCONN | El extremo de transporte ya está conectado |
| 107 | ENOTCONN | El extremo de transporte no está conectado |
| 108 | ESHUTDOWN | No se puede enviar después del cierre del punto final de transporte |
| 109 | ETOMANYREFS | Demasiadas referencias: No se puede empalmar |
| 110 | ETIMEDOUT | Tiempo de espera de conexión agotado |
| 111 | ECONNREFUSED | Conexión rechazada |
| 112 | EHOSTDOWN | El host está inactivo |
| 113 | EHOSTUNREACH | No hay ruta al host |
| 114 | EALREADY | Operación ya en curso |
| 115 | EINPROGRESS | Operación ahora en curso |
| 116 | | |

| Número de error | Código de error | Significado |
|-----------------|-----------------|--|
| 117 | EUCLEAN | La estructura necesita limpieza |
| 118 | ENOTNAM | No es un archivo de tipo con nombre XENIX |
| 119 | ENAVAIL | No hay semáforos en XENIX disponibles |
| 120 | EISNAM | Es un archivo de tipo con nombre |
| 121 | EREMOTEIO | Error de E/S remota |
| 122 | EDQUOT | Se superó la cuota |
| 123 | ENOMIUM | No se ha encontrado ningún medio |
| 124 | EMEDIUMTYPE | Tipo de medio incorrecto |
| 125 | ECANCELED | Operación cancelada |
| 126 | ENOKEY | Llave requerida no disponible |
| 127 | EKEYEXPIRED | La clave ha caducado |
| 128 | EKEYREVOKED | La llave se ha revocado |
| 129 | EKEYREJECTED | El servicio técnico ha rechazado la clave |
| 130 | EOWNERDEAD | Para los mutex robustos: El dueño murió |
| 131 | ENOPTECOMERABLE | Para los mutex robustos: El Estado no es recuperable |

Configurar la gestión de registros y el servidor syslog externo

Consideraciones que tener en cuenta sobre el uso de un servidor de syslog externo

Un servidor de syslog externo es un servidor fuera de StorageGRID que se puede utilizar para recopilar información de auditoría del sistema en una sola ubicación. El uso de un servidor de syslog externo permite reducir el tráfico de red en los nodos de administrador y gestionar la información de manera más eficiente. Para StorageGRID, el formato de paquete de mensajes syslog de salida es compatible con RFC 3164.

Los tipos de información de auditoría que se pueden enviar al servidor de syslog externo incluyen:

- Los registros de auditoría que contienen mensajes de auditoría generados durante el funcionamiento

normal del sistema

- Eventos relacionados con la seguridad, como inicios de sesión y escalados a root
- Registros de la aplicación que se pueden solicitar si es necesario abrir un caso de soporte para solucionar un problema con el que se ha encontrado

Cuándo usar un servidor de syslog externo

Un servidor syslog externo es especialmente útil si tiene un grid grande, utiliza varios tipos de aplicaciones S3 o desea conservar todos los datos de auditoría. El envío de información de auditoría a un servidor de syslog externo permite:

- Recopile y gestione información de auditoría como mensajes de auditoría, registros de aplicaciones y eventos de seguridad de forma más eficaz.
- Reduzca el tráfico de red de los nodos de administrador, ya que la información de auditoría se transfiere directamente desde los diversos nodos de almacenamiento al servidor de syslog externo, sin tener que pasar por un nodo de administración.



Cuando se envían los registros a un servidor de syslog externo, al final del mensaje se truncan los registros individuales de más de 8.192 bytes para cumplir con las limitaciones comunes en las implementaciones de servidores de syslog externos.



Para maximizar las opciones de recuperación completa de datos en caso de fallo del servidor syslog externo, ('localaudit.log`se mantienen hasta 20 GB de registros locales de registros de auditoría) en cada nodo.

Cómo configurar un servidor de syslog externo

Para aprender a configurar un servidor syslog externo, consulte "["Configurar la gestión de registros y el servidor syslog externo"](#).

Si planea configurar el uso del protocolo TLS o RELP/TLS, debe tener los siguientes certificados:

- **Certificados de CA de servidor:** Uno o más certificados de CA de confianza para verificar el servidor syslog externo en codificación PEM. Si se omite, se utilizará el certificado de CA de cuadrícula predeterminado.
- **Certificado de cliente:** El certificado de cliente para la autenticación al servidor syslog externo en codificación PEM.
- **Clave privada de cliente:** Clave privada para el certificado de cliente en codificación PEM.



Si utiliza un certificado de cliente, también debe usar una clave privada de cliente. Si proporciona una clave privada cifrada, también debe proporcionar la contraseña. No hay ninguna ventaja de seguridad significativa por el uso de una clave privada cifrada, ya que la clave y la frase de contraseña deben almacenarse; se recomienda usar una clave privada no cifrada, si está disponible, para facilitar la utilización.

Cómo calcular el tamaño del servidor de syslog externo

Normalmente, el tamaño de su grid se ajusta para lograr el rendimiento requerido, definido en términos de operaciones de S3 por segundo o bytes por segundo. Por ejemplo, es posible que exista un requisito de que su grid gestione 1,000 operaciones de S3 por segundo, o 2,000 MB por segundo, de gestión de contenidos y

recuperaciones de objetos. Se debe ajustar el tamaño del servidor de syslog externo de acuerdo con los requisitos de datos de la cuadrícula.

En esta sección, se proporcionan algunas fórmulas heurísticas que ayudan a calcular la tasa y el tamaño medio de los mensajes de registro de distintos tipos que debe ser capaz de gestionar el servidor de syslog externo, expresadas en términos de las características de rendimiento conocidas o deseadas de la cuadrícula (operaciones de S3 por segundo).

Use las operaciones de S3 por segundo en fórmulas de estimación

Si se ha ajustado el tamaño de un grid para un rendimiento expresado en bytes por segundo, debe convertir este tamaño en operaciones de S3 por segundo para utilizar las fórmulas de estimación. Para convertir el rendimiento del grid, primero debe determinar el tamaño medio del objeto, que puede utilizar la información de los registros de auditoría y las métricas existentes (si las hubiera), o utilizar sus conocimientos de las aplicaciones que utilizarán StorageGRID. Por ejemplo, si se ha ajustado el tamaño de la cuadrícula para conseguir un rendimiento de 2,000 MB/segundo y el tamaño medio del objeto es de 2 MB, el tamaño de la cuadrícula fue capaz de gestionar 1,000 operaciones de S3 por segundo (2,000 MB/2 MB).



Las fórmulas para el ajuste de tamaño del servidor de syslog externo en las siguientes secciones proporcionan estimaciones de casos comunes (en lugar de estimaciones con respecto a los peores casos). Según la configuración y la carga de trabajo, es posible que se vea una tasa mayor o menor de mensajes de syslog o volumen de datos de syslog que las fórmulas predicen. Las fórmulas se han diseñado para utilizarse únicamente como directrices.

Fórmulas de estimación para registros de auditoría

Si no tiene información sobre la carga de trabajo de S3 distinta al número de operaciones de S3 por segundo que se espera compatibilidad con la cuadrícula, puede calcular el volumen de registros de auditoría que tendrá que gestionar el servidor de syslog externo mediante las siguientes fórmulas. En el supuesto de que deja los niveles de auditoría establecidos en los valores predeterminados (todas las categorías se establecen en normal, excepto almacenamiento, que se establece en error):

```
Audit Log Rate = 2 x S3 Operations Rate  
Audit Log Average Size = 800 bytes
```

Por ejemplo, si el tamaño del grid se ajusta a 1,000 operaciones de S3 por segundo, el tamaño del servidor de syslog externo debe admitir 2,000 mensajes de syslog por segundo y debe poder recibir (y, por lo general, almacenar) datos de registro de auditoría a una tasa de 1.6 MB por segundo.

Si conoce más acerca de su carga de trabajo, es posible realizar estimaciones más precisas. En el caso de los registros de auditoría, las variables adicionales más importantes son el porcentaje de operaciones S3 que son PUT (frente a GET) y el tamaño medio, en bytes, de los siguientes S3 campos (las abreviaturas de 4 caracteres que se utilizan en la tabla son los nombres de los campos de registro de auditoría):

| Codificación | Campo | Descripción |
|--------------|---|---|
| SACC | Nombre de cuenta de inquilino de S3 (remitente de la solicitud) | El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas. |

| Codificación | Campo | Descripción |
|--------------|--|---|
| SBAC | Nombre de cuenta de inquilino de S3 (propietario del bloque) | El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo. |
| S3BK | S3 cucharón | El nombre de bloque de S3. |
| S3KY | Tecla S3 | El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo. |

Usemos P para representar el porcentaje de las operaciones de S3 que se sitúan, donde $0 \leq P \leq 1$ (por lo que para una carga de trabajo PUT del 100 %, $P = 1$ y para un 100 % DE CARGA de trabajo GET, $P = 0$).

Usemos K para representar el tamaño promedio de la suma de los S3 nombres de cuenta, S3 bucket y S3 key. Supongamos que el nombre de cuenta S3 es siempre mi cuenta s3 (13 bytes), los bloques tienen nombres de longitud fija como /my/Application/bucket-12345 (28 bytes) y los objetos tienen claves de longitud fija como 5733a5d7-f069-41ef-8fdb-13247494c69c (36 bytes). A continuación, el valor de K es 90 (13+13+28+36).

Si puede determinar valores para P y K, puede calcular el volumen de registros de auditoría que tendrá que manejar el servidor de syslog externo con las siguientes fórmulas, en el supuesto de que deja los niveles de auditoría establecidos en los valores predeterminados (todas las categorías establecidas en normal, excepto almacenamiento, Que está establecido en error):

$$\begin{aligned} \text{Audit Log Rate} &= ((2 \times P) + (1 - P)) \times \text{S3 Operations Rate} \\ \text{Audit Log Average Size} &= (570 + K) \text{ bytes} \end{aligned}$$

Por ejemplo, si el tamaño de su grid se define para 1,000 operaciones de S3 por segundo, su carga de trabajo será del 50 % put y sus nombres de cuentas de S3, nombres de bloques Y los nombres de objetos tienen un promedio de 90 bytes, el tamaño del servidor de syslog externo debe ser compatible con 1,500 mensajes de syslog por segundo y debe poder recibir (y almacenar normalmente) datos de registro de auditoría a una velocidad de aproximadamente 1 MB por segundo.

Fórmulas de estimación para niveles de auditoría no predeterminados

En las fórmulas proporcionadas para los registros de auditoría se asume el uso de la configuración predeterminada del nivel de auditoría (todas las categorías se establecen en normal, excepto almacenamiento, que está establecido en error). Las fórmulas detalladas para estimar la tasa y el tamaño medio de los mensajes de auditoría para los valores de nivel de auditoría no predeterminados no están disponibles. Sin embargo, la siguiente tabla se puede utilizar para hacer una estimación aproximada de la tasa; puede utilizar la fórmula de tamaño medio proporcionada para los registros de auditoría, pero tenga en cuenta que es probable que resulte en una sobreestimación porque los mensajes de auditoría adicionales son, en promedio, más pequeños que los mensajes de auditoría predeterminados.

| Condición | Fórmula |
|--|---|
| Replicación: Todos los niveles de auditoría están establecidos en Depurar o normal | Tasa de registro de auditoría = 8 x S3 Tasa de operaciones |
| Código de borrado: Todos los niveles de auditoría están establecidos en Depurar o normal | Utilice la misma fórmula que para la configuración predeterminada |

Fórmulas de estimación para eventos de seguridad

Los eventos de seguridad no están correlacionados con las operaciones de S3 y suelen producir un volumen insignificante de registros y datos. Por estas razones, no se proporcionan fórmulas de estimación.

Fórmulas de estimación para registros de aplicaciones

Si no tiene información acerca de la carga de trabajo de S3 distinta a la cantidad de operaciones de S3 por segundo que se espera compatibilidad con la cuadrícula, puede calcular el volumen de las aplicaciones que registra el servidor de syslog externo mediante las siguientes fórmulas:

Application Log Rate = 3.3 x S3 Operations Rate

Application Log Average Size = 350 bytes

Por lo tanto, si el tamaño del grid se ajusta para 1,000 operaciones de S3 por segundo, el tamaño del servidor de syslog externo debe ser compatible con 3,300 registros de aplicaciones por segundo y poder recibir (y almacenar) datos de registro de aplicaciones a una velocidad de aproximadamente 1.2 MB por segundo.

Si conoce más acerca de su carga de trabajo, es posible realizar estimaciones más precisas. Para los registros de aplicaciones, las variables adicionales más importantes son la estrategia de protección de datos (replicación frente a codificación de borrado), el porcentaje de S3 operaciones que se realizan (frente a GET/Other) y el tamaño medio, en bytes, de los siguientes S3 campos (las abreviaturas de 4 caracteres utilizadas en la tabla son los nombres de campos de registro de auditoría):

| Codificación | Campo | Descripción |
|--------------|---|---|
| SACC | Nombre de cuenta de inquilino de S3 (remitente de la solicitud) | El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas. |
| SBAC | Nombre de cuenta de inquilino de S3 (propietario del bloque) | El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo. |
| S3BK | S3 cucharón | El nombre de bloque de S3. |

| Codificación | Campo | Descripción |
|--------------|----------|---|
| S3KY | Tecla S3 | El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo. |

Ejemplo de estimaciones de tamaño

En esta sección se explican casos de ejemplo de cómo utilizar las fórmulas de estimación para cuadrículas con los siguientes métodos de protección de datos:

- Replicación
- Codificación de borrado

Si utiliza replicación para la protección de datos

Permita que P represente el porcentaje de las operaciones de S3 que put, donde $0 \leq P \leq 1$ (de modo que para una carga de trabajo PUT del 100 %, $P = 1$ y para una carga de trabajo DEL 100 %, $P = 0$).

Deje que K represente el tamaño medio de la suma de los S3 nombres de cuenta, S3 bucket y S3 key. Supongamos que el nombre de cuenta S3 es siempre mi cuenta s3 (13 bytes), los bloques tienen nombres de longitud fija como /my/Application/bucket-12345 (28 bytes) y los objetos tienen claves de longitud fija como 5733a5d7-f069-41ef-8fdb-13247494c69c (36 bytes). A continuación, K tiene un valor de 90 (13+13+28+36).

Si puede determinar valores para P y K , puede calcular el volumen de registros de aplicaciones que tendrá que manejar el servidor de syslog externo con las siguientes fórmulas.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x K))) Bytes
```

Por lo tanto, si, por ejemplo, el tamaño de su grid se ajusta a 1,000 operaciones de S3 por segundo, su carga de trabajo tiene un 50 % de sitúa y los nombres de cuentas, los nombres de bloques y los nombres de objetos de S3 tienen un promedio de 90 bytes, el tamaño de su servidor de syslog externo debe ser compatible con 1800 registros de aplicaciones por segundo, Y recibirá (y, normalmente, almacenará) datos de aplicaciones a una velocidad de 0.5 MB por segundo.

Si utiliza códigos de borrado para protección de datos

Permita que P represente el porcentaje de las operaciones de S3 que put, donde $0 \leq P \leq 1$ (de modo que para una carga de trabajo PUT del 100 %, $P = 1$ y para una carga de trabajo DEL 100 %, $P = 0$).

Deje que K represente el tamaño medio de la suma de los S3 nombres de cuenta, S3 bucket y S3 key. Supongamos que el nombre de cuenta S3 es siempre mi cuenta s3 (13 bytes), los bloques tienen nombres de longitud fija como /my/Application/bucket-12345 (28 bytes) y los objetos tienen claves de longitud fija como 5733a5d7-f069-41ef-8fdb-13247494c69c (36 bytes). A continuación, K tiene un valor de 90 (13+13+28+36).

Si puede determinar valores para P y K , puede calcular el volumen de registros de aplicaciones que tendrá que manejar el servidor de syslog externo con las siguientes fórmulas.

```

Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 + (0.9 x K))) Bytes

```

Así pues, por ejemplo, si el grid tiene el tamaño de 1.000 S3 operaciones por segundo, su carga de trabajo será del 50 % PUTS y los nombres de sus S3 cuentas, nombres de bloques, además, los nombres de objetos tienen un promedio de 90 bytes, el tamaño de su servidor syslog externo debe ser compatible con 2.250 registros de aplicación por segundo y debería poder recibir (y normalmente almacenar) datos de la aplicación a una velocidad de 0,6 MB por segundo.

Configurar la gestión de registros

Según sea necesario, configure los niveles de auditoría, los encabezados de protocolo y la ubicación de los mensajes y registros de auditoría.

Todos los nodos de StorageGRID generan mensajes de auditoría y registros para rastrear la actividad y los eventos del sistema. Los mensajes y registros de auditoría son herramientas esenciales para la supervisión y la solución de problemas.

Opcionalmente, puedes ["configurar un servidor syslog externo"](#) para guardar información de auditoría de forma remota. El uso de un servidor externo minimiza el impacto en el rendimiento del registro de mensajes de auditoría sin reducir la integridad de los datos de auditoría. Un servidor syslog externo es especialmente útil si tiene una red grande, utiliza múltiples tipos de aplicaciones S3 o desea conservar todos los datos de auditoría.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una ["navegador web compatible"](#).
- Usted tiene el ["Permiso de mantenimiento o acceso raíz"](#).
- Si planea configurar un servidor syslog externo, ha revisado y seguido las ["consideraciones que tener en cuenta sobre el uso de un servidor de syslog externo"](#).
- Si planea configurar un servidor de syslog externo con el protocolo TLS o RELP/TLS, tendrá los certificados de CA de servidor y de cliente requeridos, así como la clave privada de cliente.

Cambiar los niveles de mensajes de auditoría

Se puede establecer un nivel de auditoría diferente para cada una de las siguientes categorías de mensajes en el registro de auditoría:

| Categoría de auditoría | Configuración predeterminada | Más información |
|------------------------|------------------------------|---|
| Sistema | Normal | "Mensajes de auditoría del sistema" |
| Reducida | Error | "Mensajes de auditoría del almacenamiento de objetos" |
| Gestión | Normal | "Mensaje de auditoría de gestión" |

| Categoría de auditoría | Configuración predeterminada | Más información |
|------------------------|------------------------------|--|
| El cliente lee | Normal | " El cliente lee los mensajes de auditoría " |
| Escrituras del cliente | Normal | " El cliente escribe mensajes de auditoría " |
| ILM | Normal | " Mensajes de auditoría de ILM " |
| Replicación entre grid | Error | " CGRR: Solicitud de Replicación de Cuadrícula Cruzada " |



Durante las actualizaciones, las configuraciones de nivel de auditoría no serán efectivas de inmediato.

Pasos

1. Seleccione **Configuración > Monitoreo > Administración de registros**.
2. Para cada categoría de mensaje de auditoría, seleccione un nivel de auditoría de la lista desplegable:

| Nivel de auditoría | Descripción |
|--------------------|--|
| Apagado | No se registran mensajes de auditoría de la categoría. |
| Error | Sólo se registran los mensajes de error: mensajes de auditoría para los cuales el código de resultado no fue "exitoso" (SUCS). |
| Normal | Se registran los mensajes transaccionales estándar: Los mensajes que aparecen en estas instrucciones para la categoría. |
| Depurar | Obsoleto. Este nivel se comporta como el nivel de auditoría normal. |

Los mensajes incluidos para cualquier nivel particular incluyen los que se registrarán en los niveles superiores. Por ejemplo, el nivel normal incluye todos los mensajes de error.



Si no necesita un registro detallado de las operaciones de lectura del cliente para sus aplicaciones S3, cambie opcionalmente la configuración **Lecturas del cliente a Error** para disminuir la cantidad de mensajes de auditoría registrados en el registro de auditoría.

3. Seleccione **Guardar**.

Definir cabeceras de solicitud HTTP

Opcionalmente, puede definir cualquier encabezado de solicitud HTTP que desee incluir en los mensajes de auditoría de lectura y escritura del cliente.

Pasos

1. En la sección **Cabeceras de protocolo de auditoría**, defina los encabezados de solicitud HTTP que

desea incluir en los mensajes de auditoría de lectura y escritura del cliente.

Utilice un asterisco (*) como comodín para que coincida con cero o más caracteres. Utilice la secuencia de escape (*) para que coincida con un asterisco literal.

2. Seleccione **Agregar otro encabezado** para crear encabezados adicionales, si es necesario.

Cuando se encuentran encabezados HTTP en una solicitud, se incluyen en el mensaje de auditoría en el campo HTRH.



Los encabezados de solicitud de protocolo de auditoría se registran solo si el nivel de auditoría para **Lecturas de cliente** o **Escrituras de cliente** no está **Desactivado**.

3. Seleccione **Guardar**

Configurar la ubicación del registro

De forma predeterminada, los mensajes de auditoría y los registros se guardan en los nodos donde se generan. Se rotan periódicamente y finalmente se eliminan para evitar que consuman demasiado espacio en disco. Si desea guardar mensajes de auditoría y un subconjunto de registros de forma externa,[utilizar un servidor syslog externo](#) .

Si desea guardar los archivos de registro internamente, elija un inquilino y un depósito para el almacenamiento de registros y habilite el archivado de registros.

Utilice un servidor syslog externo

De manera opcional, es posible configurar un servidor de syslog externo para guardar registros de auditoría, registros de aplicaciones y registros de eventos de seguridad en una ubicación fuera del grid.



Si no desea utilizar un servidor syslog externo, omita este paso y vaya a [Seleccionar la ubicación del registro](#) .



Si las opciones de configuración disponibles en este procedimiento no son lo suficientemente flexibles para satisfacer sus requisitos, se pueden aplicar opciones de configuración adicionales mediante los audit-destinations puntos finales, que se encuentran en la sección API privada de ["API de gestión de grid"](#). Por ejemplo, puede usar la API si desea usar diferentes servidores de syslog para diferentes grupos de nodos.

Introduzca la información de syslog

Acceda al asistente Configurar servidor de syslog externo y proporcione la información que StorageGRID necesita para acceder al servidor de syslog externo.

Pasos

1. Desde la pestaña Nodo local y servidor externo, seleccione **Configurar servidor syslog externo**. O bien, si ha configurado previamente un servidor syslog externo, seleccione **Editar servidor syslog externo**.

Aparece el asistente Configurar servidor de syslog externo.

2. Para el paso **Enter syslog info** del asistente, introduzca un nombre de dominio completo válido o una dirección IPv4 o IPv6 para el servidor syslog externo en el campo **Host**.

3. Introduzca el puerto de destino en el servidor de syslog externo (debe ser un entero entre 1 y 65535). El puerto predeterminado es 514.
4. Seleccione el protocolo utilizado para enviar información de auditoría al servidor de syslog externo.

Se recomienda usar **TLS** o **RELP/TLS**. Debe cargar un certificado de servidor para usar cualquiera de estas opciones. El uso de certificados ayuda a proteger las conexiones entre el grid y el servidor de syslog externo. Para obtener más información, consulte "["Gestionar certificados de seguridad"](#)".

Todas las opciones de protocolo requieren compatibilidad con el servidor de syslog externo y su configuración. Debe elegir una opción que sea compatible con el servidor de syslog externo.



El protocolo de registro de eventos fiable (RELP) amplía la funcionalidad del protocolo syslog para proporcionar una entrega fiable de los mensajes de eventos. El uso de RELP puede ayudar a evitar la pérdida de información de auditoría si el servidor syslog externo tiene que reiniciarse.

5. Seleccione **continuar**.

6. Si seleccionó **TLS** o **RELP/TLS**, cargue los certificados de CA del servidor, el certificado de cliente y la clave privada del cliente.
 - a. Seleccione **Buscar** para el certificado o la clave que deseé utilizar.
 - b. Seleccione el certificado o el archivo de claves.
 - c. Seleccione **Abrir** para cargar el archivo.

Aparece una comprobación verde junto al certificado o el nombre del archivo de claves, notificándole que se ha cargado correctamente.

7. Seleccione **continuar**.

Permite gestionar el contenido de syslog

Puede seleccionar la información que desea enviar al servidor de syslog externo.

Pasos

1. Para el paso **Administrar contenido syslog** del asistente, seleccione cada tipo de información de auditoría que deseé enviar al servidor syslog externo.
 - **Enviar registros de auditoría:** Envía eventos StorageGRID y actividades del sistema
 - **Enviar eventos de seguridad:** Envía eventos de seguridad como cuando un usuario no autorizado intenta iniciar sesión o un usuario inicia sesión como root
 - **Enviar registros de aplicaciones:** Envía "[Archivos de registro del software de StorageGRID](#)" útiles para la solución de problemas, incluyendo:
 - `broadcast-err.log`
 - `broadcast.log`
 - `jaeger.log`
 - `nms.log` (Solo nodos de administración)
 - `prometheus.log`
 - `raft.log`

- `hagroups.log`
 - **Enviar registros de acceso:** Envía registros de acceso HTTP para solicitudes externas a Grid Manager, Tenant Manager, endpoints de equilibrio de carga configurados y solicitudes de federación de grid desde sistemas remotos.
2. Utilice los menús desplegables para seleccionar la gravedad y la utilidad (tipo de mensaje) para cada categoría de información de auditoría que deseé enviar.

La definición de valores de gravedad y de utilidad puede ayudarle a agregar los registros de formas personalizables para facilitar el análisis.

- a. Para **Gravedad**, selecciona **Passthrough**, o selecciona un valor de gravedad entre 0 y 7.

Si selecciona un valor, el valor seleccionado se aplicará a todos los mensajes de este tipo. La información sobre diferentes gravedades se perderá si se sustituye la gravedad por un valor fijo.

| Gravedad | Descripción |
|---------------|--|
| Paso a través | Cada mensaje enviado al syslog externo para tener el mismo valor de gravedad que cuando se registró localmente en el nodo: <ul style="list-style-type: none"> • Para los registros de auditoría, la gravedad es «info». • Para eventos de seguridad, los valores de gravedad se generan en la distribución de Linux en los nodos. • Para los registros de aplicaciones, las gravedades varían entre “info” y “notice”, dependiendo de cuál sea el problema. Por ejemplo, agregar un servidor NTP y configurar un grupo de alta disponibilidad proporciona un valor de «info», mientras que detener intencionalmente el servicio SSM o RSM proporciona un valor de «notice». • Para los registros de acceso, la gravedad es «info». |
| 0 | Emergencia: El sistema no se puede utilizar |
| 1 | Alerta: La acción se debe realizar de inmediato |
| 2 | Crítico: Condiciones críticas |
| 3 | Error: Condiciones de error |
| 4 | Advertencia: Condiciones de aviso |
| 5 | Aviso: Condición normal pero significativa |
| 6 | Informativo: Mensajes informativos |
| 7 | Debug: Mensajes de nivel de depuración |

- b. Para **Facility**, selecciona **Passthrough**, o selecciona un valor entre 0 y 23.

Si selecciona un valor, se aplicará a todos los mensajes de este tipo. La información sobre las diferentes instalaciones se perderá si se sustituye la instalación por un valor fijo.

| Centro | Descripción |
|---------------|--|
| Paso a través | <p>Cada mensaje enviado al syslog externo para tener el mismo valor de instalación que cuando se registró localmente en el nodo:</p> <ul style="list-style-type: none"> • Para los registros de auditoría, la instalación enviada al servidor de syslog externo es «local7». • Para los eventos de seguridad, los valores de las instalaciones se generan mediante la distribución de linux en los nodos. • Para los registros de aplicaciones, los registros de aplicaciones enviados al servidor syslog externo tienen los siguientes valores de utilidad: <ul style="list-style-type: none"> ◦ bycast.log: usuario o daemon ◦ bycast-err.log: usuario, daemon, local3 o local4 ◦ jaeger.log: local2 ◦ nms.log: local3 ◦ prometheus.log: local4 ◦ raft.log: local5 ◦ hagroups.log: local6 • Para los registros de acceso, la instalación enviada al servidor syslog externo es “local0”. |
| 0 | kern (mensajes del núcleo) |
| 1 | usuario (mensajes de usuario) |
| 2 | correo |
| 3 | daemon (daemons del sistema) |
| 4 | auth (mensajes de seguridad/autorización) |
| 5 | syslog (mensajes generados internamente por syslogd) |
| 6 | lpr (subsistema de impresora de líneas) |
| 7 | noticias (subsistema de noticias de red) |
| 8 | UCP |
| 9 | cron (daemon de reloj) |

| Centro | Descripción |
|---------------|--|
| 10 | seguridad (mensajes de seguridad/autorización) |
| 11 | FTP |
| 12 | NTP |
| 13 | auditoría de registro (auditoría de registros) |
| 14 | alerta de registro (alerta de registro) |
| 15 | reloj (daemon de reloj) |
| 16 | local0 |
| 17 | local1 |
| 18 | local2 |
| 19 | local3 |
| 20 | local4 |
| 21 | local5 |
| 22 | local6 |
| 23 | local7 |

3. Seleccione **continuar**.

Enviar mensajes de prueba

Antes de iniciar el uso de un servidor de syslog externo, debe solicitar que todos los nodos de la cuadrícula envíen mensajes de prueba al servidor de syslog externo. Se deben usar estos mensajes de prueba para ayudar a validar toda la infraestructura de recogida de registros antes de comprometerse a enviar datos al servidor de syslog externo.

 No use la configuración del servidor de syslog externo hasta que confirme que el servidor de syslog externo recibió un mensaje de prueba de cada nodo del grid y que el mensaje se procesó como se esperaba.

Pasos

1. Si no desea enviar mensajes de prueba porque está seguro de que su servidor syslog externo está configurado correctamente y puede recibir información de auditoría de todos los nodos de la cuadrícula, seleccione **Omitir y finalizar**.

Un banner verde indica que se ha guardado la configuración.

2. De lo contrario, seleccione **Enviar mensajes de prueba** (recomendado).

Los resultados de la prueba aparecen continuamente en la página hasta que se detiene la prueba. Mientras la prueba está en curso, los mensajes de auditoría siguen enviarse a los destinos configurados anteriormente.

3. Si recibe algún error durante la configuración del servidor syslog o en el tiempo de ejecución, corríjalo y seleccione **Enviar mensajes de prueba** nuevamente.

Consulte "[Solucione problemas de un servidor de syslog externo](#)" para ayudarle a resolver cualquier error.

4. Espere hasta que vea un banner verde que indica que todos los nodos han superado la prueba.

5. Compruebe el servidor de syslog para determinar si se reciben y procesan los mensajes de prueba según lo esperado.



Si está utilizando UDP, verifique toda su infraestructura de recopilación de registros. El protocolo UDP no permite una detección de errores tan rigurosa como los otros protocolos.

6. Seleccione **Detener y finalizar**.

Volverá a la página **Audit and syslog Server**. Un banner de color verde indica que se guardó la configuración del servidor de syslog.



La información de auditoría de StorageGRID no se envía al servidor syslog externo hasta que seleccione un destino que incluya el servidor syslog externo.

Seleccionar la ubicación del registro

Puede especificar dónde se guardan los registros de auditoría y los registros de eventos de seguridad. "[Registros de aplicaciones de StorageGRID](#)", y se envían registros de acceso.

StorageGRID toma por defecto los destinos de auditoría de nodo local y almacena la información de auditoría en `/var/local/log/localaudit.log`.

Al utilizar `/var/local/log/localaudit.log`, las entradas del registro de auditoría de Grid Manager y Tenant Manager se pueden enviar a un nodo de almacenamiento. Puede encontrar el nodo que tiene las entradas más recientes mediante `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"` el comando.

Algunos destinos solo están disponibles si se configuró un servidor de syslog externo.

Pasos

1. Seleccione **Ubicación del registro > Nodo local y servidor externo**.

2. Para cambiar la ubicación del registro para los tipos de registro, seleccione una opción diferente.



Solo nodos locales y Servidor syslog externo típicamente proporcionan un mejor rendimiento.

| Opción | Descripción |
|---|---|
| Sólo Nodos Locales (valor por defecto) | <p>Los mensajes de auditoría, los registros de eventos de seguridad y los registros de aplicaciones no se envían a los nodos de administración. En cambio, se guardan únicamente en los nodos que los generaron ("el nodo local"). La información de auditoría generada en cada nodo local se almacena en <code>/var/local/log/localaudit.log</code>.</p> <p>Nota: StorageGRID elimina periódicamente los registros locales en una rotación para liberar espacio. Cuando el archivo de registro de un nodo alcanza 1 GB, se guarda el archivo existente y se inicia un nuevo archivo de registro. El límite de rotación del registro es de 21 archivos. Cuando se crea la versión 22 del archivo de registro, se elimina el archivo de registro más antiguo. En promedio, se almacenan alrededor de 20 GB de datos de registro en cada nodo. Para almacenar registros durante un período de tiempo prolongado,Utilice un inquilino y un depósito para el almacenamiento de registros .</p> |
| Nodos de administración/nodos locales | <p>Los mensajes de auditoría se envían al registro de auditoría en los nodos de administración, y los registros de eventos de seguridad y los registros de aplicaciones se almacenan en los nodos que los generaron. La información de auditoría se almacena en los siguientes archivos:</p> <ul style="list-style-type: none"> • 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> archivo suele estar vacío o faltar. Puede contener información secundaria, como una copia adicional de algunos mensajes. |
| Servidor de syslog externo | <p>La información de auditoría se envía a un servidor syslog externo y se guarda en los nodos locales(<code>/var/local/log/localaudit.log</code>). El tipo de información enviada depende de cómo haya configurado el servidor syslog externo. Esta opción se habilita solo después de haberconfiguró un servidor syslog externo .</p> |
| Nodos de administración y servidor syslog externo | <p>Los mensajes de auditoría se envían al registro de auditoría.(<code>/var/local/audit/export/audit.log</code>) en los nodos de administración y la información de auditoría se envía al servidor syslog externo y se guarda en el nodo local(<code>/var/local/log/localaudit.log</code>). El tipo de información enviada depende de cómo haya configurado el servidor syslog externo. Esta opción se habilita solo después de haberconfiguró un servidor syslog externo .</p> |

3. Seleccione Guardar.

Aparecerá un mensaje de advertencia.

4. Seleccione **OK** para confirmar que desea cambiar el destino para la información de auditoría.

Los nuevos registros se envían a los destinos seleccionados. Los registros existentes permanecen en su ubicación actual.

Usa un cubo

Los registros se rotan periódicamente. Utilice un bucket S3 en la misma red para almacenar registros durante un período de tiempo prolongado.

1. Seleccione **Ubicación del registro > Usar un depósito**.
2. Seleccione la casilla de verificación **Habilitar registros de archivo**.
3. Si el inquilino y el depósito enumerados no son los que desea utilizar, seleccione **Cambiar inquilino y depósito** y luego seleccione **Crear inquilino y depósito** o **Seleccionar inquilino y depósito**.

Crear inquilino y depósito

- a. Introduzca un nuevo nombre de inquilino.
- b. Ingrese y confirme una contraseña para el nuevo inquilino.
- c. Introduzca un nuevo nombre de depósito.
- d. Seleccione **Crear y habilitar**.

Seleccione tenant and bucket

- a. Seleccione un nombre de inquilino del menú desplegable.
- b. Seleccione un depósito del menú desplegable.
- c. Seleccione **Seleccionar y habilitar**.

4. Seleccione **Guardar**.

Los registros se almacenarán en el inquilino y en el depósito que usted especifique. El nombre de la clave del objeto para los registros tiene este formato:

```
system-logs/{node_hostname}/{absolute_path_to_log_file_on_node}--  
{last_modified_time}.gz
```

Por ejemplo:

```
system-logs/DC1-SN1/var/local/log/localaudit.log--2025-05-12_13:41:44.gz
```

Usar supervisión de SNMP

Usar supervisión de SNMP

Si desea supervisar StorageGRID mediante el protocolo simple de gestión de redes (SNMP), debe configurar el agente SNMP que se incluye con StorageGRID.

- "Configure el agente SNMP"
- "Actualice el agente SNMP"

Funcionalidades

Cada nodo StorageGRID ejecuta un agente SNMP, o demonio, que proporciona una MIB. La MiB de StorageGRID contiene definiciones de tabla y notificaciones para alertas. El MIB también contiene información de descripción del sistema, como la plataforma y el número de modelo de cada nodo. Cada nodo StorageGRID también admite un subconjunto de objetos MIB-II.



Consulte "[Acceda a los archivos MIB](#)" si desea descargar los archivos MIB en los nodos de grid.

Inicialmente, SNMP está deshabilitado en todos los nodos. Al configurar el agente SNMP, todos los nodos StorageGRID reciben la misma configuración.

El agente SNMP de StorageGRID admite las tres versiones del protocolo SNMP. Proporciona acceso MIB de solo lectura para consultas, y puede enviar dos tipos de notificaciones condicionadas por eventos a un sistema de gestión:

Trampas

Las trampas son notificaciones enviadas por el agente SNMP que no requieren reconocimiento por parte del sistema de gestión. Los traps sirven para notificar al sistema de gestión que algo ha sucedido dentro de StorageGRID, por ejemplo, que se activa una alerta.

Las tres versiones de SNMP admiten capturas.

Informa

Los informes son similares a las capturas, pero requieren el reconocimiento del sistema de gestión. Si el agente SNMP no recibe una confirmación dentro de un cierto período de tiempo, vuelve a enviar la información hasta que se reciba una confirmación o se haya alcanzado el valor máximo de reintento.

Los informes son compatibles con SNMPv2c y SNMPv3.

Las notificaciones Trap e INFORM se envían en los siguientes casos:

- Una alerta predeterminada o personalizada se activa en cualquier nivel de gravedad. Para suprimir las notificaciones SNMP correspondientes a una alerta, debe "[configurar un silencio](#)" aparecer como la alerta. Las notificaciones de alerta son enviadas por el "[Nodo de administración de remitente preferido](#)".

Cada alerta se asigna a uno de los tres tipos de trampa según el nivel de gravedad de la alerta: ActiveMinorAlert, activeMajorAlert y activeCriticalAlert. Para obtener una lista de las alertas que pueden activar estos solapamientos, consulte la "[Referencia de alertas](#)".

Compatibilidad con versiones de SNMP

La tabla proporciona un resumen a grandes rasgos de lo que se admite para cada versión de SNMP.

| | SNMPv1 | SNMPv2c | SNMPv3 |
|---|---|---|--|
| Consultas (OBTENER y GETNEXT) | Consultas MIB de solo lectura | Consultas MIB de solo lectura | Consultas MIB de solo lectura |
| Consulta de autenticación | Cadena de comunidad | Cadena de comunidad | Usuario del modelo de seguridad basado en el usuario (USM) |
| Notificaciones (ATRAPAR e INFORMAR) | Sólo capturas | Atrapa e informa | Atrapa e informa |
| Autenticación de notificaciones | Comunidad de capturas predeterminada o una cadena de comunidad personalizada para cada destino de capturas | Comunidad de capturas predeterminada o una cadena de comunidad personalizada para cada destino de capturas | Usuario USM en cada destino de captura |

Limitaciones

- StorageGRID admite acceso MIB de solo lectura. No se admite el acceso de lectura y escritura.
- Todos los nodos de la cuadrícula reciben la misma configuración.
- SNMPv3: StorageGRID no admite el modo de soporte para transporte (TSM).
- SNMPv3: El único protocolo de autenticación compatible es SHA (HMAC-SHA-96).
- SNMPv3: El único protocolo de privacidad compatible es AES.

Configure el agente SNMP

Es posible configurar el agente SNMP de StorageGRID para que use un sistema de gestión SNMP de terceros para el acceso a MIB de solo lectura y las notificaciones.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Usted tiene el "[Permiso de acceso raíz](#)".

Acerca de esta tarea

El agente SNMP de StorageGRID admite SNMPv1, SNMPv2c y SNMPv3. Puede configurar el agente para una o más versiones. Para SNMPv3, solo se admite la autenticación con modelos de seguridad de usuario (USM).

Todos los nodos del grid utilizan la misma configuración SNMP.

Especifique la configuración básica

Como primer paso, habilite el agente SMNP de StorageGRID y proporcione información básica.

Pasos

1. Seleccione **Configuración > Monitoreo > Agente SNMP**.

Aparece la página del agente SNMP.

2. Para habilitar el agente SNMP en todos los nodos de la cuadrícula, seleccione la casilla de verificación **Activar SNMP**.

3. Introduzca la siguiente información en la sección Configuración básica.

| Campo | Descripción |
|--|--|
| Contacto del sistema | Opcional. El contacto principal del sistema StorageGRID, que se devuelve en mensajes de SNMP como sysContact. El contacto del sistema suele ser una dirección de correo electrónico. Este valor se aplica a todos los nodos del sistema StorageGRID. El contacto del sistema puede tener un máximo de 255 caracteres. |
| Ubicación del sistema | Opcional. La ubicación del sistema StorageGRID, que se devuelve en mensajes de SNMP como sysLocation. La ubicación del sistema puede ser cualquier información útil para identificar dónde se encuentra el sistema StorageGRID. Por ejemplo, puede utilizar la dirección de una instalación. Este valor se aplica a todos los nodos del sistema StorageGRID. La ubicación del sistema puede tener un máximo de 255 caracteres. |
| Activar notificaciones de agente SNMP | <ul style="list-style-type: none">Si se selecciona, el agente SNMP de StorageGRID envía notificaciones de captura e información.Si no se selecciona, el agente SNMP admite el acceso MIB de solo lectura, pero no envía ninguna notificación SNMP. |
| Habilite las capturas de autenticación | Si se selecciona, el agente SNMP de StorageGRID envía capturas de autenticación si recibe mensajes de protocolo autenticados incorrectamente. |

Introduzca las cadenas de comunidad

Si usa SNMPv1 o SNMPv2c, complete la sección Community Strings.

Cuando el sistema de gestión consulta el MIB de StorageGRID, envía una cadena de comunidad. Si la cadena de comunidad coincide con uno de los valores especificados aquí, el agente SNMP envía una respuesta al sistema de administración.

Pasos

1. Para **Comunidad de solo lectura**, opcionalmente, introduzca una cadena de comunidad para permitir el acceso MIB de solo lectura en las direcciones de agente IPv4 y IPv6.



Para garantizar la seguridad de su sistema StorageGRID, no utilice «public» como cadena de comunidad. Si deja este campo vacío, el agente SNMP utiliza el identificador de grid del sistema StorageGRID como la cadena de comunidad.

Cada cadena de comunidad puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

2. Seleccione **Agregar otra cadena de comunidad** para agregar cadenas adicionales.

Se permiten hasta cinco cadenas.

Crear destinos de capturas

Use la pestaña Destinos de captura en la sección Otras configuraciones para definir uno o más destinos para las notificaciones de captura StorageGRID o Inform. Cuando habilita el agente SNMP y selecciona **Guardar**, StorageGRID envía notificaciones a cada destino definido cuando se activan alertas. También se envían notificaciones estándar para las entidades MIB-II admitidas (por ejemplo, ifdown y coldStart).

Pasos

1. Para el campo **default trap community**, opcionalmente, introduzca la cadena de comunidad predeterminada que desea utilizar para destinos de captura SNMPv1 o SNMPv2.

Según sea necesario, puede proporcionar una cadena de comunidad diferente (personalizada) al definir un destino de captura específico.

La comunidad de capturas predeterminada puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

2. Para agregar un destino de captura, selecciona **Crear**.
3. Seleccione la versión de SNMP que se utilizará para este destino de capturas.
4. Complete el formulario Crear destino de captura para la versión seleccionada.

SNMPv1

Si seleccionó SNMPv1 como versión, complete estos campos.

| Campo | Descripción |
|---------------------|--|
| Tipo | Debe ser Trampa para SNMPv1. |
| Host | Una dirección IPv4 o IPv6, o un nombre de dominio completo (FQDN) para recibir la captura. |
| Puerto | Utilice 162, que es el puerto estándar para capturas de SNMP a menos que tenga que usar otro valor. |
| Protocolo | Utilice UDP, que es el protocolo de captura SNMP estándar a menos que necesite utilizar TCP. |
| Cadena de comunidad | <p>Use la comunidad de capturas predeterminada, si se especificó una o introduzca una cadena de comunidad personalizada para este destino de captura.</p> <p>La cadena de comunidad personalizada puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.</p> |

SNMPv2c

Si seleccionó SNMPv2c como versión, complete estos campos.

| Campo | Descripción |
|---------------------|--|
| Tipo | Si el destino se utilizará para trampas o informes. |
| Host | Una dirección IPv4 o IPv6 o un FQDN para recibir la captura. |
| Puerto | Utilice 162, que es el puerto estándar para capturas de SNMP a menos que se deba usar otro valor. |
| Protocolo | Utilice UDP, que es el protocolo de captura SNMP estándar a menos que necesite utilizar TCP. |
| Cadena de comunidad | <p>Use la comunidad de capturas predeterminada, si se especificó una o introduzca una cadena de comunidad personalizada para este destino de captura.</p> <p>La cadena de comunidad personalizada puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.</p> |

SNMPv3

Si seleccionó SNMPv3 como versión, complete estos campos.

| Campo | Descripción |
|-------------|--|
| Tipo | Si el destino se utilizará para trampas o informes. |
| Host | Una dirección IPv4 o IPv6 o un FQDN para recibir la captura. |
| Puerto | Utilice 162, que es el puerto estándar para capturas de SNMP a menos que se deba usar otro valor. |
| Protocolo | Utilice UDP, que es el protocolo de captura SNMP estándar a menos que necesite utilizar TCP. |
| Usuario USM | <p>El usuario USM que se usará para la autenticación.</p> <ul style="list-style-type: none"> • Si ha seleccionado Trap, sólo se mostrarán los usuarios USM sin identificación de motor autorizada. • Si ha seleccionado INFORM, sólo se mostrarán los usuarios USM con ID de motor autoritativos. • Si no se muestran usuarios: <ul style="list-style-type: none"> i. Cree y guarde el destino de captura. ii. Vaya a Crear usuarios USM y cree el usuario. iii. Vuelva a la pestaña Destinos de solapamiento, seleccione el destino guardado de la tabla y seleccione Editar. iv. Seleccione el usuario. |

5. Seleccione **Crear**.

El destino de captura se crea y se añade a la tabla.

Crear direcciones de agente

Opcionalmente, utilice el separador Direcciones de Agente de la sección Otras configuraciones para especificar una o más direcciones de recepción. Estas son las direcciones StorageGRID en las que el agente SNMP puede recibir consultas.

Si no configura una dirección de agente, la dirección de recepción predeterminada es el puerto UDP 161 en todas las redes StorageGRID.

Pasos

1. Seleccione **Crear**.
2. Introduzca la siguiente información.

| Campo | Descripción |
|-------------------------|--|
| Protocolo de Internet | <p>Si esta dirección usará IPv4 o IPv6.</p> <p>De forma predeterminada, SNMP utiliza IPv4.</p> |
| Protocolo de transporte | <p>Si esta dirección usará UDP o TCP.</p> <p>De forma predeterminada, SNMP utiliza UDP.</p> |
| Red StorageGRID | <p>En qué red StorageGRID escuchará el agente.</p> <ul style="list-style-type: none"> • Redes Grid, Admin y Client: El agente SNMP escuchará las consultas en las tres redes. • Red Grid • Red de administración • Red cliente <p>Nota: Si utiliza la Red de clientes para datos inseguros y crea una dirección de agente para la Red de clientes, tenga en cuenta que el tráfico SNMP también será inseguro.</p> |
| Puerto | <p>Opcionalmente, el número de puerto en el que debe recibir el agente SNMP.</p> <p>El puerto UDP predeterminado para un agente SNMP es 161, pero puede introducir cualquier número de puerto no utilizado.</p> <p>Nota: Al guardar el agente SNMP, StorageGRID abre automáticamente los puertos de dirección del agente en el firewall interno. Debe asegurarse de que cualquier firewall externo permita el acceso a estos puertos.</p> |

3. Seleccione **Crear**.

La dirección del agente se crea y se agrega a la tabla.

Crear usuarios USM

Si utiliza SNMPv3, use la pestaña Usuarios USM en la sección Otras configuraciones para definir los usuarios de USM que están autorizados a consultar la MIB o recibir capturas e informar.



Para los destinos *trap* de SNMPv3, se recomienda crear un usuario USM para cada nodo de administración. Si cada nodo de administración no tiene un usuario USM, su sistema de administración podría dejar de recibir notificaciones si el nodo de administración principal deja de funcionar.



SNMPv3 *Inform* Los destinos deben tener usuarios con ID de motor. El destino *trap* de SNMPv3 no puede tener usuarios con ID de motor.

Estos pasos no se aplican si solo usas SNMPv1 o SNMPv2c.

Pasos

1. Seleccione **Crear**.
2. Introduzca la siguiente información.

| Campo | Descripción |
|---------------------------------|--|
| Nombre de usuario | <p>Nombre único para este usuario USM.</p> <p>Los nombres de usuario pueden tener un máximo de 32 caracteres y no pueden contener espacios en blanco. El nombre de usuario no se puede cambiar después de crear el usuario.</p> |
| Acceso a la MIB de solo lectura | <p>Si se selecciona, este usuario debe tener acceso de solo lectura a la MIB.</p> |
| ID de motor autorizado | <p>Si este usuario se va a utilizar en un destino de informe, el ID de motor autorizado para este usuario.</p> <p>Introduzca de 10 a 64 caracteres hexadecimales (de 5 a 32 bytes) sin espacios. Este valor es obligatorio para los usuarios de USM que se seleccionarán en destinos de captura para los informes. Este valor no está permitido para los usuarios de USM que se seleccionarán en destinos de captura para capturas.</p> <p>Nota: Este campo no se muestra si seleccionaste Acceso MIB de solo lectura porque los usuarios USM que tienen acceso MIB de solo lectura no pueden tener ID de motor.</p> |
| Nivel de seguridad | <p>Nivel de seguridad del usuario USM:</p> <ul style="list-style-type: none">• Authpriv: Este usuario se comunica con autenticación y privacidad (cifrado). Debe especificar un protocolo y una contraseña de autenticación, y un protocolo y una contraseña de privacidad.• AuthNoprivilegios: Este usuario se comunica con autenticación y sin privacidad (sin cifrado). Debe especificar un protocolo de autenticación y una contraseña. |
| Protocolo de autenticación | Siempre configurado en SHA, que es el único protocolo compatible (HMAC-SHA-96). |
| Contraseña | Contraseña que utilizará este usuario para la autenticación. |
| Protocolo de privacidad | Solo se muestra si seleccionó AUTHPRIV y siempre se establece en AES, que es el único protocolo de privacidad compatible. |
| Contraseña | Solo se muestra si seleccionaste AUTHPRIV . La contraseña que este usuario utilizará para la privacidad. |

3. Seleccione **Crear**.

El usuario USM se crea y se añade a la tabla.

4. Cuando haya completado la configuración del agente SNMP, seleccione **Guardar**.

La nueva configuración del agente SNMP se activa.

Actualice el agente SNMP

Es posible deshabilitar notificaciones SNMP, actualizar cadenas de comunidad, o añadir o quitar direcciones de agentes, usuarios de USM y destinos de capturas.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Usted tiene el "[Permiso de acceso raíz](#)".

Acerca de esta tarea

Consulte "[Configure el agente SNMP](#)" para obtener detalles sobre cada campo en la página del agente SNMP. Debe seleccionar **Guardar** en la parte inferior de la página para confirmar los cambios que realice en cada pestaña.

Pasos

1. Seleccione **Configuración > Monitoreo > Agente SNMP**.

Aparece la página del agente SNMP.

2. Para desactivar el agente SNMP en todos los nodos de la cuadrícula, desactive la casilla de verificación **Habilitar SNMP** y seleccione **Guardar**.

Si vuelve a habilitar el agente SNMP, se conservan todos los ajustes de configuración anteriores de SNMP.

3. Si lo desea, actualice la información en la sección Configuración básica:

- a. Según sea necesario, actualice el **Contacto del sistema y Ubicación del sistema**.
- b. Opcionalmente, seleccione o desactive la casilla de verificación **Activar notificaciones de agente SNMP** para controlar si el agente SNMP de StorageGRID envía notificaciones de trap e informen.

Cuando esta casilla de comprobación está desactivada, el agente SNMP admite el acceso MIB de solo lectura, pero no envía notificaciones SNMP.

- c. Opcionalmente, seleccione o desactive la casilla de verificación **Habilitar capturas de autenticación** para controlar si el agente SNMP de StorageGRID envía capturas de autenticación cuando recibe mensajes de protocolo autenticados incorrectamente.

4. Si usa SNMPv1 o SNMPv2c, opcionalmente actualice o agregue una **comunidad de solo lectura** en la sección de cadenas de comunidad.

5. Para actualizar los destinos de capturas, seleccione la pestaña Destinos de captura en la sección Otras configuraciones.

Utilice esta pestaña para definir uno o más destinos para las notificaciones de captura StorageGRID o Inform. Cuando habilita el agente SNMP y selecciona **Guardar**, StorageGRID envía notificaciones a cada destino definido cuando se activan alertas. También se envían notificaciones estándar para las entidades

MIB-II admitidas (por ejemplo, ifdown y coldStart).

Para obtener más información sobre qué introducir, consulte "[Cree destinos de capturas](#)".

- Opcionalmente, actualice o elimine la comunidad de capturas predeterminada.

Si quita la comunidad de capturas predeterminada, primero debe asegurarse de que todos los destinos de capturas existentes utilicen una cadena de comunidad personalizada.

- Para agregar un destino de captura, selecciona **Crear**.
- Para editar un destino de captura, seleccione el botón de opción y seleccione **Editar**.
- Para eliminar un destino de captura, seleccione el botón de opción y seleccione **Eliminar**.
- Para confirmar los cambios, selecciona **Guardar** en la parte inferior de la página.

6. Para actualizar las direcciones del agente, seleccione el separador Direcciones del agente en la sección Otras configuraciones.

Utilice esta pestaña para especificar una o más direcciones de recepción. Estas son las direcciones StorageGRID en las que el agente SNMP puede recibir consultas.

Para obtener más información sobre qué introducir, consulte "[Crear direcciones de agente](#)".

- Para agregar una dirección de agente, selecciona **Crear**.
- Para editar una dirección de agente, seleccione el botón de opción y seleccione **Editar**.
- Para eliminar una dirección de agente, seleccione el botón de opción y seleccione **Eliminar**.
- Para confirmar los cambios, selecciona **Guardar** en la parte inferior de la página.

7. Para actualizar usuarios de USM, seleccione la pestaña USM users en la sección Otras configuraciones.

Use esta pestaña para definir los usuarios USM que están autorizados a consultar el MIB o a recibir capturas e informes.

Para obtener más información sobre qué introducir, consulte "[Crear usuarios USM](#)".

- Para agregar un usuario USM, selecciona **Crear**.
- Para editar un usuario USM, seleccione el botón de opción y seleccione **Editar**.

No se puede cambiar el nombre de usuario de USM existente. Si necesita cambiar un nombre de usuario, debe eliminar el usuario y crear uno nuevo.



Si agrega o elimina el ID de motor autorizado de un usuario y ese usuario está seleccionado actualmente para un destino, debe editar o eliminar el destino. De lo contrario, se produce un error de validación al guardar la configuración del agente SNMP.

- Para eliminar un usuario USM, seleccione el botón de opción y seleccione **Eliminar**.



Si el usuario que eliminó está seleccionado actualmente para un destino de captura, debe editar o eliminar el destino. De lo contrario, se produce un error de validación al guardar la configuración del agente SNMP.

- Para confirmar los cambios, selecciona **Guardar** en la parte inferior de la página.

8. Cuando haya actualizado la configuración del agente SNMP, seleccione **Guardar**.

Acceda a los archivos MIB

Los archivos MIB contienen definiciones e información sobre las propiedades de los recursos y servicios gestionados para los nodos en el grid. Es posible acceder a los archivos MIB que definen los objetos y las notificaciones para StorageGRID. Estos archivos pueden ser útiles para supervisar la cuadrícula.

Consulte "[Usar supervisión de SNMP](#)" para obtener más información acerca de los archivos SNMP y MIB.

Acceda a los archivos MIB

Siga estos pasos para acceder a los archivos MIB.

Pasos

1. Seleccione **Configuración > Monitoreo > Agente SNMP**.
2. En la página del agente SNMP, seleccione el archivo que deseé descargar:
 - **NETAPP-STORAGEGRID-MIB.txt**: Define la tabla de alertas y las notificaciones (traps) a las que se puede acceder en todos los nodos de administración.
 - **ES-NETAPP-06-MIB.mib**: Define objetos y notificaciones para dispositivos basados en E-Series.
 - **MIB_1_10.zip**: Define objetos y notificaciones para dispositivos con interfaz BMC.



También puede acceder a los archivos MIB en la siguiente ubicación en cualquier nodo StorageGRID: /usr/share/snmp/mibs

3. Para extraer los OID de StorageGRID del archivo MIB:

- a. Obtenga el OID de la raíz de la MIB de StorageGRID:

```
root@user-adm1:~ # snmptranslate -On -IR storagegrid
```

Resultado: .1.3.6.1.4.1.789.28669 (28669 Es siempre el OID de StorageGRID)

- b. Grep para el OID de StorageGRID en todo el árbol (utilizando paste para unir líneas):

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



El `snmptranslate` comando tiene muchas opciones que son útiles para explorar la MIB. Este comando está disponible en cualquier nodo StorageGRID.

Contenido del archivo MIB

Todos los objetos están bajo el OID de StorageGRID.

| Nombre del objeto | ID Objeto (OID) | Descripción |
|-------------------|-----------------|--|
| | | Módulo MIB para entidades de NetApp StorageGRID. |

Objetos MIB

| Nombre del objeto | ID Objeto (OID) | Tipo | Acceso | Módulo MIB | Descripción |
|--------------------------|-----------------|-------------------------------|--------------|------------------------|--|
| Active AlertCount | | Integer32 | Sólo lectura | NETAPP-STORAGEGRID-MIB | El número de alertas activas en activeAlertTable. |
| Active AlertTable | | Secuencia de ActiveAlertEntry | No accesible | NETAPP-STORAGEGRID-MIB | Una tabla de alertas activas en StorageGRID. |
| Entrada de alerta activa | | Secuencia | No accesible | NETAPP-STORAGEGRID-MIB | Una única alerta de StorageGRID , indexada por ID de alerta. |
| Active AlertId | | Cadena de octetos | Sólo lectura | NETAPP-STORAGEGRID-MIB | El ID de la alerta. Solo es único en el conjunto actual de alertas activas. |
| Active AlertName | | Cadena de octetos | Sólo lectura | NETAPP-STORAGEGRID-MIB | El nombre de la alerta. |
| Active AlertInstance | | Cadena de octetos | Sólo lectura | NETAPP-STORAGEGRID-MIB | El nombre de la entidad que generó la alerta, generalmente el nombre del nodo. |
| Active AlertSeverity | | Cadena de octetos | Sólo lectura | NETAPP-STORAGEGRID-MIB | La gravedad de la alerta. |
| Active AlertStartTime | | Fecha y hora | Sólo lectura | NETAPP-STORAGEGRID-MIB | La hora en que se activó la alerta. |

Recopilación de datos de StorageGRID adicionales

SUPERVISE EL RENDIMIENTO DE PUT y GET

Puede supervisar el rendimiento de ciertas operaciones, como el almacén de objetos y la recuperación, para ayudar a identificar los cambios que podrían requerir una investigación adicional.

Acerca de esta tarea

Para supervisar el rendimiento de PUT y GET, puede ejecutar comandos S3 directamente desde una estación de trabajo o mediante la aplicación S3tester de código abierto. El uso de estos métodos permite evaluar el rendimiento independientemente de factores externos a StorageGRID, como problemas con una aplicación

cliente o problemas con una red externa.

Al realizar pruebas de PUT Y GET Operations, siga estas directrices:

- Utilice tamaños de objetos comparables a los objetos que se suelen procesar en el grid.
- Realice operaciones tanto en sitios locales como remotos.

Los mensajes del "registro de auditoría" indican el tiempo total necesario para ejecutar determinadas operaciones. Por ejemplo, para determinar el tiempo de procesamiento total de una solicitud GET de S3, puede revisar el valor del atributo TIME en el mensaje de auditoría SGET. También puede encontrar el atributo TIME en los mensajes de auditoría para las siguientes S3 operaciones: DELETE, GET, HEAD, Metadata Updated, POST, PUT

Al analizar los resultados, observe el tiempo medio necesario para satisfacer una solicitud, así como el rendimiento general que puede obtener. Repita las mismas pruebas regularmente y registre los resultados, para que pueda identificar tendencias que podrían requerir investigación.

- Puede ["Descargue el probador S3 del github"](#).

Supervise las operaciones de verificación de objetos

El sistema StorageGRID puede verificar la integridad de los datos de objetos en los nodos de almacenamiento, comprobando si hay objetos dañados o ausentes.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una ["navegador web compatible"](#).
- Usted tiene el ["Permiso de mantenimiento o acceso raíz"](#).

Acerca de esta tarea

Dos ["procesos de verificación"](#) trabajan juntos para garantizar la integridad de los datos:

- **La verificación en segundo plano** se ejecuta automáticamente, comprobando continuamente la corrección de los datos del objeto.

La verificación en segundo plano comprueba de forma automática y continua todos los nodos de almacenamiento para determinar si hay copias dañadas de los datos de objetos replicados y codificados para borrado. Si se encuentran problemas, el sistema StorageGRID intenta automáticamente reemplazar los datos de objetos dañados de las copias almacenadas en otro lugar del sistema. La verificación en segundo plano no se ejecuta en objetos de un Cloud Storage Pool.



La alerta **Objeto corrupto no identificado detectado** se activa si el sistema detecta un objeto corrupto que no se puede corregir automáticamente.

- **La comprobación de la existencia de objetos** puede ser desencadenada por un usuario para verificar más rápidamente la existencia (aunque no la corrección) de los datos del objeto.

La comprobación de existencia de objetos verifica si todas las copias replicadas esperadas de objetos y fragmentos codificados con borrado existen en un nodo de almacenamiento. La comprobación de la existencia de objetos proporciona una forma de verificar la integridad de los dispositivos de almacenamiento, especialmente si un problema de hardware reciente podría haber afectado a la integridad de los datos.

Debe revisar regularmente los resultados de las verificaciones de fondo y las comprobaciones de la existencia de objetos. Investigue inmediatamente cualquier instancia de datos de objeto dañados o que faltan para determinar la causa raíz.

Pasos

1. Revise los resultados de las verificaciones de fondo:

- a. Seleccione **Nodos > Nodo de almacenamiento > Objetos**.

- b. Compruebe los resultados de verificación:

- Para comprobar la verificación de datos de objetos replicados, observe los atributos de la sección verificación.

| Verification | | |
|-------------------------------|-----------------------|--|
| Status: | No errors | |
| Percent complete: | 0.00% | |
| Average stat time: | 0.00 microseconds | |
| Objects verified: | 0 | |
| Object verification rate: | 0.00 objects / second | |
| Data verified: | 0 bytes | |
| Data verification rate: | 0.00 bytes / second | |
| Missing objects: | 0 | |
| Corrupt objects: | 0 | |
| Corrupt objects unidentified: | 0 | |
| Quarantined objects: | 0 | |

- Para comprobar la verificación de fragmentos codificados por borrado, seleccione **Storage Node > ILM** y observe los atributos de la sección verificación de códigos de borrado.

Erasure coding verification

| | | |
|---------------------------------------|-------------------------|--|
| Status: ? | Idle | |
| Next scheduled: ? | 2021-10-08 10:45:19 MDT | |
| Fragments verified: ? | 0 | |
| Data verified: ? | 0 bytes | |
| Corrupt copies: ? | 0 | |
| Corrupt fragments: ? | 0 | |
| Missing fragments: ? | 0 | |

Seleccione el signo de interrogación [?](#) junto al nombre de un atributo para mostrar el texto de ayuda.

2. Revise los resultados de los trabajos de comprobación de la existencia de objetos:
 - a. Seleccione **Mantenimiento > Comprobación de existencia de objetos > Historial de trabajos**.
 - b. Escanee la columna Copias de objetos faltantes detectadas. Si alguno de los trabajos generó 100 o más copias de objetos faltantes y se activó la alerta **Objetos potencialmente perdidos**, comuníquese con el soporte técnico.

Object existence check

Perform an object existence check if you suspect storage volumes have been damaged or are corrupt. You can verify objects defined by your ILM policy, still exist on the volumes.

[Active job](#) [Job history](#)

[Delete](#)

| <input type="checkbox"/> | Job ID ? | Status | Nodes (volumes) ? | Missing object copies detected ? |
|--------------------------|--------------------------|-----------|--|--|
| <input type="checkbox"/> | 15816859223101303015 | Completed | DC2-S1 (3 volumes) | 0 |
| <input type="checkbox"/> | 12538643155010477372 | Completed | DC1-S3 (1 volume) | 0 |
| <input type="checkbox"/> | 5490044849774982476 | Completed | DC1-S2 (1 volume) | 0 |
| <input type="checkbox"/> | 3395284277055907678 | Completed | DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and 7 more | 0 |

Revisar los mensajes de auditoría

Los mensajes de auditoría pueden ayudarle a comprender mejor las operaciones detalladas del sistema StorageGRID. Es posible usar registros de auditoría para solucionar problemas y evaluar el rendimiento.

Durante el funcionamiento normal del sistema, todos los servicios de StorageGRID generan mensajes de auditoría de la siguiente manera:

- Los mensajes de auditoría del sistema están relacionados con el mismo sistema de auditoría, los estados del nodo de grid, la actividad de tareas en todo el sistema y las operaciones de backup de servicio.
- Los mensajes de auditoría del almacenamiento de objetos están relacionados con el almacenamiento y la gestión de objetos dentro de StorageGRID, incluidos el almacenamiento y la recuperación de objetos, el nodo de grid a nodos de grid y las verificaciones.
- Los mensajes de auditoría de lectura y escritura del cliente se registran cuando una aplicación cliente S3 realiza una solicitud para crear, modificar o recuperar un objeto.
- Los mensajes de auditoría de gestión registran las solicitudes de los usuarios a la API de gestión.

Cada nodo de administración almacena los mensajes de auditoría en archivos de texto. El recurso compartido de auditoría contiene el archivo activo (audit.log) y registros de auditoría comprimidos de los días anteriores. Cada nodo de la cuadrícula también almacena una copia de la información de auditoría generada en el nodo.

Puede acceder a los archivos log de auditoría directamente desde la línea de comandos del nodo de administración.

StorageGRID puede enviar información de auditoría de forma predeterminada o cambiar el destino:

- StorageGRID se establece de forma predeterminada en destinos de auditoría de nodo local.
- Las entradas del registro de auditoría de Grid Manager y Tenant Manager pueden enviarse a un nodo de almacenamiento.
- De manera opcional, se puede cambiar el destino de los registros de auditoría y enviar información de auditoría a un servidor de syslog externo. Se siguen generando y almacenando registros locales de registros de auditoría cuando se configura un servidor de syslog externo.
- ["Obtenga información sobre cómo configurar la gestión de registros"](#).

Para obtener más información sobre el archivo log de auditoría, el formato de los mensajes de auditoría, los tipos de mensajes de auditoría y las herramientas disponibles para analizar los mensajes de auditoría, consulte ["Revisar los registros de auditoría"](#).

Recopilar archivos de registro y datos del sistema

Puede recuperar archivos de registro y datos del sistema de StorageGRID , incluidos los datos de configuración, y enviarlos al soporte técnico.

Antes de empezar

- Ha iniciado sesión en el Administrador de cuadrícula en cualquier nodo de administración mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).
- Tiene la clave de acceso de aprovisionamiento.

Acerca de esta tarea

Utilice el Administrador de cuadrícula para recopilar "[archivos de registro](#)" , datos del sistema y datos de configuración de cualquier nodo de la red durante el período de tiempo que seleccione. Los datos se recopilan y archivan en un `.tar.gz` archivo que luego puede descargar a su computadora local o enviar al soporte técnico.

Opcionalmente, puede cambiar el destino de los registros de auditoría y enviar información de auditoría a un servidor syslog externo. Los registros locales de registros de auditoría continúan generándose y almacenándose cuando se configura un servidor syslog externo. Ver "["Configurar la gestión de registros y el servidor syslog externo"](#)" .

Pasos

1. Seleccione **Soporte > Herramientas > Recopilación de registros**. Se muestra una tabla de nodos.

2. Seleccione los nodos de grid para los que desea recoger archivos de registro.

Puede ordenar por nombre de nodo, sitio y tipo de nodo. Las columnas de tipo de sitio y nodo contienen filtros para seleccionar por sitios individuales y tipos de nodo.

3. Seleccione **continuar**.

4. Seleccione el rango de fecha y hora de los datos que se incluirán en los archivos de registro.

Si selecciona un período de tiempo muy largo o recopila registros de todos los nodos en una cuadrícula grande, el archivo de registros podría volverse demasiado grande para almacenarse en un nodo o demasiado grande para que un nodo de administración lo recopile para descargarlo. Si ocurre cualquiera de los escenarios, reinicie la recopilación de registros con un conjunto de datos más pequeño.

5. Seleccione los tipos de registros que desea recoger.

- **Registros de aplicaciones:** registros específicos de la aplicación que el soporte técnico utiliza con mayor frecuencia para solucionar problemas. Los registros recopilados son un subconjunto de los registros de aplicaciones disponibles.
- **Registros de auditoría:** Registros que contienen los mensajes de auditoría generados durante el funcionamiento normal del sistema.
- **Rastreo de red:** registros utilizados para la depuración de red.
- **Base de datos Prometheus:** métricas de series temporales de los servicios en todos los nodos.

6. Opcionalmente, utilice el cuadro de texto **Notas** para ingresar notas sobre los archivos de registro que está recopilando.

Puede usar estas notas para brindar información de soporte técnico acerca del problema que le pidió que recopile los archivos de registro. Las notas se agregan a un archivo llamado `info.txt`, junto con otra información sobre la recopilación de archivos de registro. `'info.txt'` El archivo se guarda en el paquete de archivo de registro.

7. En el cuadro de texto **Frase de contraseña de aprovisionamiento**, ingrese la frase de contraseña de aprovisionamiento para su sistema StorageGRID .

8. Seleccione **Recopilar registros**.

Puede utilizar la página de Recopilación de registros para supervisar el progreso de la recopilación de archivos de registro para cada nodo de la cuadrícula.

Si recibe un mensaje de error acerca del tamaño del registro, intente recopilar registros por un período más corto de tiempo o para menos nodos.

9. Si falla la recopilación de registros:

- Si aparece el mensaje "Error en la recopilación de registros", puede volver a intentar la recopilación de registros o finalizar la sesión sin volver a intentarlo.
- Si aparece el mensaje "La recopilación de registros falló parcialmente", puede volver a intentar la recopilación de registros, finalizar la sesión, descargar el archivo de registro parcial o enviar el archivo de registro parcial a AutoSupport.

10. Cuando se complete la recopilación de archivos de registro:

- Seleccione **Descargar** para descargar el .tar.gz archivo.
- Seleccione **Enviar a AutoSupport** para enviar el .tar.gz archivo al soporte técnico.

El .tar.gz El archivo contiene todos los archivos de registro de todos los nodos de la red donde la recopilación de registros fue exitosa. El combinado .tar.gz El archivo contiene un archivo de registro para cada nodo de la red.

El tema del paquete AutoSupport es USER_TRIGGERED_SUPPORT_BUNDLE .

11. Seleccione **Finalizar**.



El .tar.gz El archivo se elimina cuando selecciona **Finalizar**. Asegúrese de descargar o enviar el archivo primero.

Active manualmente un paquete AutoSupport

Para ayudar al soporte técnico en la solución de problemas con el sistema StorageGRID, puede activar manualmente el envío de un paquete AutoSupport.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Tienes acceso de root u otro permiso de configuración de red.

Pasos

1. Seleccione **Soporte > Herramientas > * AutoSupport***.
2. En la pestaña **Acciones**, selecciona **Enviar AutoSupport activado por el usuario**.

StorageGRID intenta enviar un paquete de AutoSupport al sitio de soporte de NetApp . Si el intento es exitoso, se actualizan los valores **Resultado más reciente** y **Última vez exitoso** en la pestaña **Resultados**. Si hay un problema, el valor **Resultado más reciente** se actualiza a "Error" y StorageGRID no intenta enviar el paquete AutoSupport nuevamente.

3. Después de 1 minuto, actualice la página de AutoSupport en su navegador para acceder a los resultados más recientes.



Además, puedes "[Recopilar archivos de registro y datos del sistema más extensos](#)" y envíelos al sitio de soporte de NetApp .

Revisar las métricas de soporte

Al solucionar problemas, puede trabajar con el soporte técnico para revisar métricas y gráficos detallados para su sistema StorageGRID.

Antes de empezar

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

Acerca de esta tarea

La página Metrics le permite acceder a las interfaces de usuario Prometheus y Grafana. Prometheus es un software de código abierto para recopilar métricas. Grafana es un software de código abierto para la visualización de métricas.



Las herramientas disponibles en la página Métricas están destinadas al soporte técnico. Algunas funciones y elementos de menú de estas herramientas no son intencionalmente funcionales y están sujetos a cambios. Consulte la lista de "["Métricas de Prometheus que se usan habitualmente"](#)".

Pasos

1. Según las indicaciones del soporte técnico, seleccione **Soporte > Herramientas > Métricas**.

A continuación se muestra un ejemplo de la página Metrics:

Metrics

Access charts and metrics to help troubleshoot issues.

The tools on this page are for use by technical support. Some features and menu items within these tools are intentionally non-functional.

Prometheus is an open-source toolkit for collecting metrics. The Prometheus interface allows you to query the current values of metrics and to view charts of the values over time. Access the Prometheus interface using the link below. You must be signed in to the Grid Manager.

<https://>

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values. Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

| | | |
|---|--|---|
| ADE | Cloud Storage Pool Overview | Platform Services Processing |
| Account Service Overview | Decommission | Replicated Read Path Overview |
| Alertmanager | Erasure Coding - ADE | S3 - Node |
| Appliance Hardware Status | Erasure Coding - Overview | S3 Control |
| Audit Overview | Grid | S3 Overview |
| Bucket Cache | ILM | S3 Select |
| Cache Service | Identity Service Overview | Site |
| Cassandra Cluster Overview | Ingests | Support |
| Cassandra Network Overview | Node | SSD - Warranty |
| Cassandra Node Overview | Node (Internal Use) | Traces |
| Cassandra Table Cleanup | Object Chunk Leak Overview | Traffic Classification Policy |
| Chunk - Operations Overview | Object Serialization Mapping | Usage Processing |
| Chunk - Flesytem Latency Overview | OSL - AsyncIO | Virtual Memory (vmstat) |
| Chunk - Flesytem Latency Details | Platform Services Commits | |
| Cross Grid Replication | Platform Services Overview | |

2. Para consultar los valores actuales de las métricas de StorageGRID y ver gráficos de los valores a lo largo del tiempo, haga clic en el enlace de la sección Prometheus.

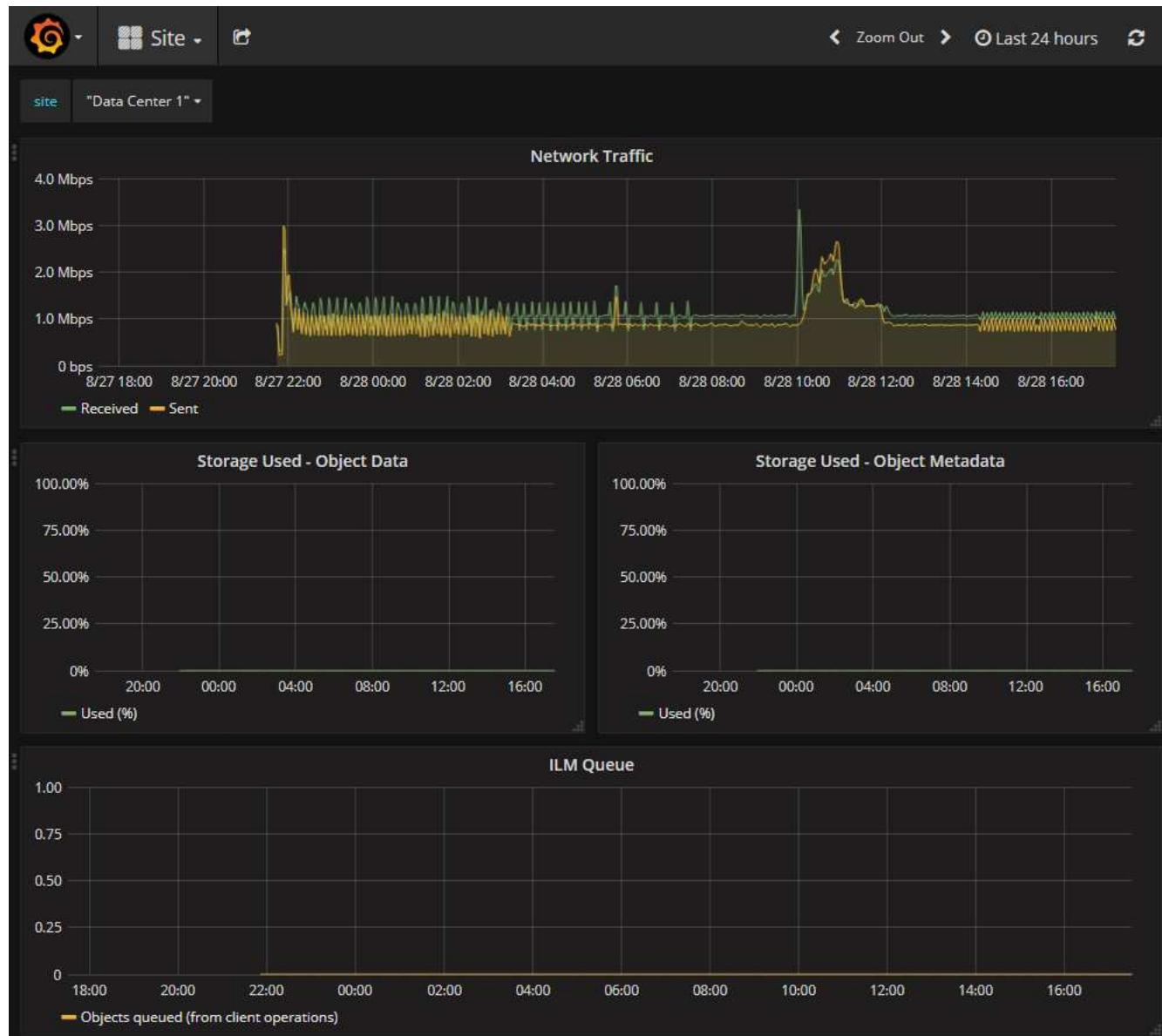
Aparece la interfaz Prometheus. Puede utilizar esta interfaz para ejecutar consultas en las métricas de StorageGRID disponibles y para generar un gráfico de las métricas de StorageGRID a lo largo del tiempo.



Las métricas que incluyen *private* en sus nombres están destinadas únicamente a uso interno y están sujetas a cambios entre versiones de StorageGRID sin previo aviso.

3. Para acceder a paneles preconstruidos que contienen gráficos de métricas de StorageGRID a lo largo del tiempo, haga clic en los enlaces de la sección Grafana.

Aparece la interfaz de Grafana para el enlace seleccionado.



Cambiar la priorización de E/S

La priorización de entrada/salida (E/S) le permite cambiar las prioridades relativas para las operaciones de E/S en la red.

De manera predeterminada, el tráfico de E/S PUT y GET del cliente recibe la máxima prioridad por sobre las actividades en segundo plano, como la purga de datos codificados por borrado (EC) y la reparación de EC. Al

aumentar la prioridad de purga de datos codificados por borrado (EC) y de las actividades de reparación de EC, estas tareas posiblemente puedan completarse más rápido. La efectividad de los cambios de priorización de E/S se ve afectada por la tasa de solicitudes de clientes, las fluctuaciones del tráfico de red y otras tareas de red en curso.

Antes de empezar

- Revise la página de priorización de E/S para determinar qué opciones podrían afectar su red.
- Evalúe si el tráfico continuo de clientes puede manejar de manera segura tiempos de espera más prolongados o tiempos de espera de clientes.
- Esté preparado para monitorear el efecto del cambio de priorización y realizar los ajustes necesarios. Estos cambios se implementan rápidamente pero sus efectos pueden tardar horas en hacerse visibles.

Pasos

1. Seleccione **Soporte > Priorización de E/S**.
2. (Opcional) Cambie la prioridad de purga y reparación de EC, para las operaciones en segundo plano que purgan datos de EC, de sus valores predeterminados.
 Utilice la prioridad de reparación y purga de CE baja predeterminada para redes que tienen nodos basados en RAID.
3. Seleccione **Guardar**.
4. Monitorear el "["métrica"](#)" para evaluar el efecto de los cambios de priorización.

Ejecutar diagnóstico

Al solucionar un problema, el soporte técnico puede trabajar para ejecutar diagnósticos del sistema StorageGRID y revisar los resultados.

- "["Revisar las métricas de soporte"](#)"
- "["Métricas de Prometheus que se usan habitualmente"](#)"

Antes de empezar

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

Acerca de esta tarea

La página Diagnósticos realiza un conjunto de comprobaciones de diagnóstico en el estado actual de la cuadrícula. Cada control de diagnóstico puede tener uno de los tres Estados:

-  **Normal:** Todos los valores están dentro del rango normal.
-  **Atención:** Uno o más de los valores están fuera del rango normal.
-  **Precaución:** Uno o más de los valores están significativamente fuera del rango normal.

Los Estados de diagnóstico son independientes de las alertas actuales y podrían no indicar problemas operativos con la cuadrícula. Por ejemplo, una comprobación de diagnóstico puede mostrar el estado Precaución aunque no se haya activado ninguna alerta.

Pasos

1. Seleccione **Soporte > Herramientas > Diagnóstico**.

Aparece la página Diagnósticos y enumera los resultados de cada comprobación de diagnóstico. Los resultados se ordenan por gravedad (Precaución, atención y luego normal). Dentro de cada gravedad, los resultados se ordenan alfabéticamente.

En este ejemplo, un diagnóstico tiene un estado de Atención y tres diagnósticos tienen un estado Normal.

The screenshot shows the 'Diagnostics' page. At the top, there are two status icons: a red circle with a white 'X' labeled 'Caution' and a yellow triangle with an exclamation mark labeled 'Attention'. Below these are the counts '0' and '1' respectively. A blue button labeled 'Run Diagnostics' is visible. The main area lists four diagnostic checks, each with a status icon and a checkmark:

- Node uptime (Attention)
- Alert silences (Normal)
- Appliance hardware component temperatures (Normal)
- Cassandra automatic restarts (Normal)

2. Para obtener más información acerca de un diagnóstico específico, haga clic en cualquier lugar de la fila.

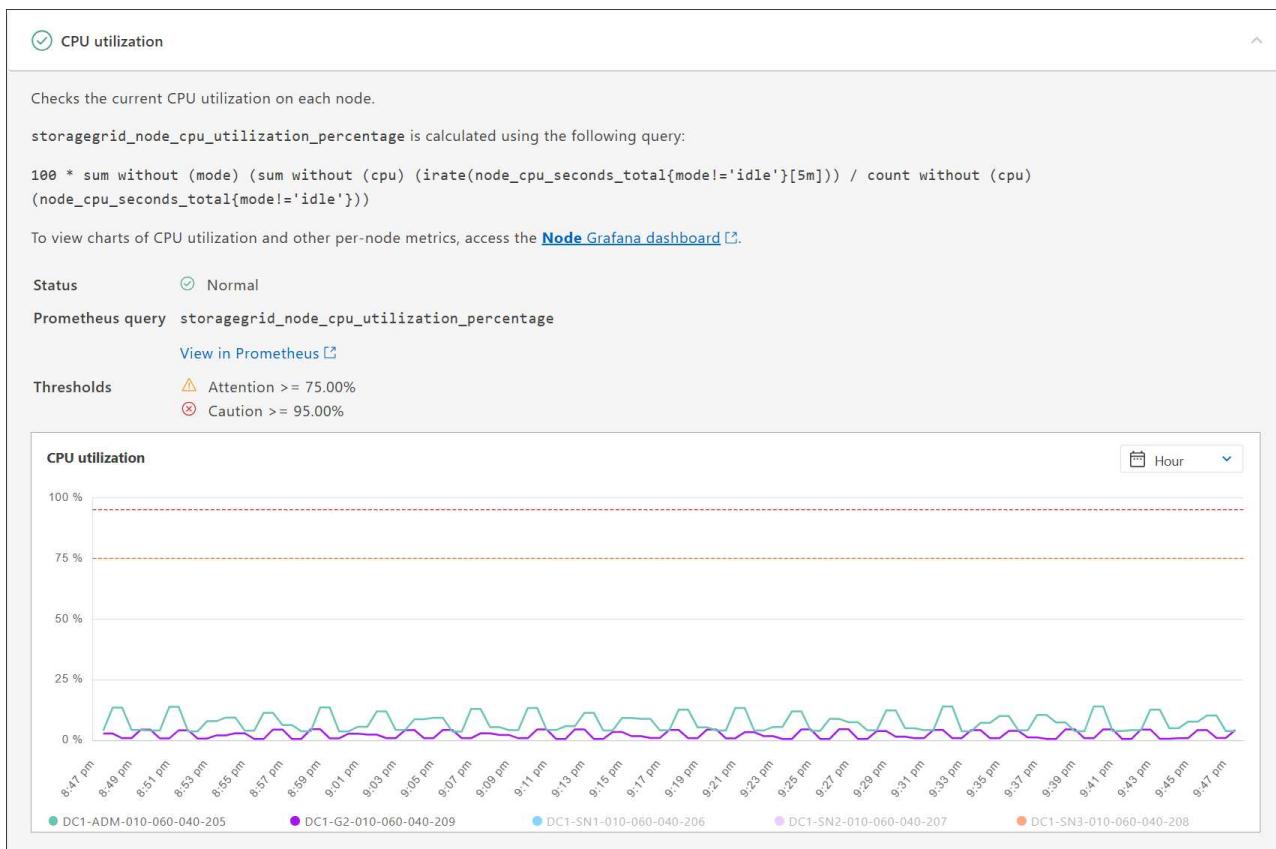
Aparecen detalles sobre el diagnóstico y sus resultados actuales. Se enumeran los siguientes detalles:

- **Estado:** El estado actual de este diagnóstico: Normal, atención o Precaución.
- **Consulta Prometheus:** Si se utiliza para el diagnóstico, la expresión Prometheus que se utilizó para generar los valores de estado. (No se utiliza una expresión Prometheus para todos los diagnósticos.)
- **Umbrales:** Si están disponibles para el diagnóstico, los umbrales definidos por el sistema para cada estado de diagnóstico anormal. (Los valores de umbral no se utilizan para todos los diagnósticos).



No puedes cambiar estos umbrales.

- **Valores de estado:** un gráfico y una tabla (tabla no mostrada en la captura de pantalla) que muestran el estado y el valor del diagnóstico en todo el sistema StorageGRID . En este ejemplo, se muestra la utilización actual de la CPU para cada nodo en un sistema StorageGRID . Todos los valores de los nodos están por debajo de los umbrales de Atención y Precaución, por lo que el estado general del diagnóstico es Normal.



3. Opcional: Para ver los gráficos de Grafana relacionados con este diagnóstico, seleccione **Panel de Grafana**.

Este enlace no se muestra para todos los diagnósticos.

Aparece el panel de Grafana relacionado. En este ejemplo, aparece el panel de control del nodo mostrando la utilización de la CPU a lo largo del tiempo para este nodo, así como otros gráficos de Grafana para el nodo.



También puede acceder a los paneles de Grafana prediseñados desde la sección Grafana de la página **Sopporte > Herramientas > Métricas**.



4. **Opcional:** Para ver un gráfico de la expresión Prometheus a lo largo del tiempo, haga clic en **Ver en Prometheus**.

Aparece un gráfico Prometheus de la expresión utilizada en el diagnóstico.

Enable query history

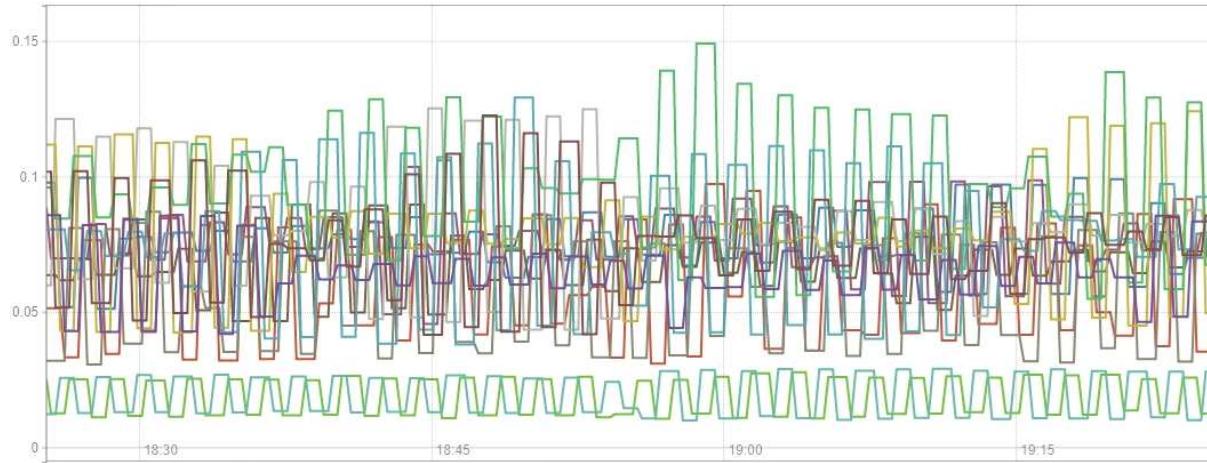
```
sum by (instance) (sum by (instance, mode) (rate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode))
```

Load time: 547ms
Resolution: 14s
Total time series: 13

Execute

- insert metric at cursor -

Graph

- 1h + ◀ Until ▶ Res. (s) stacked


- {instance="DC3-S3"}
- {instance="DC3-S2"}
- {instance="DC3-S1"}
- {instance="DC2-S3"}
- {instance="DC2-S2"}
- {instance="DC2-S1"}
- {instance="DC2-ADM1"}
- {instance="DC1-S3"}
- {instance="DC1-S2"}
- {instance="DC1-S1"}
- {instance="DC1-G1"}
- {instance="DC1-ARC1"}
- {instance="DC1-ADM1"}

Remove Graph

Add Graph

Crear aplicaciones de supervisión personalizadas

Puede crear aplicaciones y paneles de supervisión personalizados utilizando las métricas de StorageGRID disponibles en la API de gestión de grid.

Si desea supervisar las métricas que no se muestran en una página existente del gestor de grid o si desea crear paneles personalizados para StorageGRID, puede utilizar la API de gestión de grid para consultar las métricas de StorageGRID.

También puede acceder a la métrica Prometheus directamente con una herramienta de supervisión externa, como Grafana. El uso de una herramienta externa requiere que usted cargue o genere un certificado de cliente administrativo para permitir que StorageGRID autentique la herramienta para la seguridad. Consulte la ["Instrucciones para administrar StorageGRID"](#).

Para ver las operaciones de la API de métricas, incluida la lista completa de las métricas disponibles, vaya a Grid Manager. En la parte superior de la página, selecciona el ícono de ayuda y selecciona **Documentación de la API > Métricas**.

| | | | |
|-----|------------------------------------|--|--|
| GET | /grid/metric-labels/{label}/values | Lists the values for a metric label | |
| GET | /grid/metric-names | Lists all available metric names | |
| GET | /grid/metric-query | Performs an instant metric query at a single point in time | |
| GET | /grid/metric-query-range | Performs a metric query over a range of time | |

Los detalles de cómo implementar una aplicación de supervisión personalizada están fuera del alcance de esta documentación.

Solucionar los problemas del sistema StorageGRID

Solucionar los problemas de un sistema StorageGRID

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

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

Defina el problema

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

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

| Pregunta | Ejemplo de respuesta |
|--|--|
| ¿Qué está haciendo o no el sistema StorageGRID? ¿Cuáles son sus síntomas? | Las aplicaciones cliente informan de que los objetos no se pueden procesar en StorageGRID. |
| ¿Cuándo comenzó el problema? | La ingestión de objetos fue denegada por primera vez a las 14:50 del 8 de enero de 2020. |
| ¿Cómo notó el problema por primera vez? | Notificado por la aplicación cliente. También ha recibido notificaciones por correo electrónico de alerta. |
| ¿El problema ocurre de manera consistente, o sólo a veces? | El problema está en curso. |

| Pregunta | Ejemplo de respuesta |
|--|--|
| Si el problema ocurre con regularidad, ¿qué pasos hacen que ocurra | El problema se produce cada vez que un cliente intenta procesar un objeto. |
| Si el problema ocurre intermitentemente, ¿cuándo ocurre? Registre las horas de cada incidente que conozca. | El problema no es intermitente. |
| ¿Ha visto este problema con anterioridad? ¿Con qué frecuencia ha tenido este problema en el pasado? | Esta es la primera vez que veo este asunto. |

Evalué el riesgo y el impacto sobre el sistema

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

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

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

Recopilación de datos

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

| Tipo de datos que se van a recoger | Por qué recoger estos datos | Instrucciones |
|--|---|--|
| Crear una línea de tiempo de los cambios recientes | Los cambios realizados en el sistema StorageGRID, su configuración o su entorno pueden provocar nuevos comportamientos. | <ul style="list-style-type: none"> Crear una línea de tiempo de cambios recientes |

| Tipo de datos que se van a recoger | Por qué recoger estos datos | Instrucciones |
|--|---|--|
| Revisar las alertas | <p>Las alertas pueden ayudarle a determinar rápidamente la causa raíz de un problema proporcionando pistas importantes sobre los problemas subyacentes que podrían estar causando.</p> <p>Revise la lista de alertas actuales para ver si StorageGRID ha identificado la causa raíz de un problema para usted.</p> <p>Revise las alertas activadas en el pasado para obtener información adicional.</p> | <ul style="list-style-type: none"> "Ver las alertas actuales y resueltas" |
| Establecer líneas base | Recopilar información acerca de los niveles normales de varios valores operativos. Estos valores de referencia y las desviaciones de estas líneas de base pueden proporcionar pistas valiosas. | <ul style="list-style-type: none"> "Establecer líneas base" |
| Realice pruebas de procesamiento y recuperación | Para solucionar problemas de rendimiento con la ingestión y la recuperación, utilice una estación de trabajo para almacenar y recuperar objetos. Compare los resultados con los que se ven al usar la aplicación cliente. | <ul style="list-style-type: none"> "SUPERVISE EL RENDIMIENTO DE PUT y GET" |
| Revisar los mensajes de auditoría | Revise los mensajes de auditoría para seguir las operaciones de StorageGRID con detalle. Los detalles de los mensajes de auditoría pueden ser útiles para solucionar muchos tipos de problemas, incluidos problemas de rendimiento. | <ul style="list-style-type: none"> "Revisar los mensajes de auditoría" |
| Comprobar la ubicación de objetos y la integridad del almacenamiento | Si tiene problemas de almacenamiento, compruebe que los objetos se encuentren en la ubicación que espera. Compruebe la integridad de los datos de objetos en un nodo de almacenamiento. | <ul style="list-style-type: none"> "Supervise las operaciones de verificación de objetos" "Confirme las ubicaciones de los datos del objeto" "Verifique la integridad del objeto" |
| Recopile datos para el soporte técnico | Es posible que el soporte técnico le solicite recopilar datos o revisar información específica para ayudar a resolver problemas. | <ul style="list-style-type: none"> "Recopilar archivos de registro y datos del sistema" "Active manualmente un paquete AutoSupport" "Revisar las métricas de soporte" |

cree una línea de tiempo de los cambios recientes

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

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

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

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

Ejemplos de cambios recientes significativos

A continuación se muestran algunos ejemplos de cambios potencialmente importantes:

- ¿El sistema StorageGRID se ha instalado, ampliado o recuperado recientemente?
- ¿Se ha actualizado el sistema recientemente? ¿Se ha aplicado una revisión?
- ¿Se ha reparado o modificado recientemente algún hardware?
- ¿Se ha actualizado la política de ILM?
- ¿Ha cambiado la carga de trabajo del cliente?
- ¿Ha cambiado la aplicación cliente o su comportamiento?
- ¿Ha cambiado los equilibradores de carga, o ha agregado o eliminado un grupo de alta disponibilidad de nodos de administrador o nodos de puerta de enlace?
- ¿Se ha iniciado alguna tarea que puede tardar mucho tiempo en completarse? Entre los ejemplos se incluyen:
 - Recuperación de un nodo de almacenamiento con fallos
 - Decomisionado del nodo de almacenamiento
- ¿Se han realizado cambios en la autenticación de usuario, por ejemplo, añadir un inquilino o cambiar la configuración de LDAP?
- ¿Se está realizando la migración de datos?

- ¿Se han activado o cambiado los servicios de la plataforma recientemente?
- ¿Se ha activado el cumplimiento de normativas recientemente?
- ¿Se han añadido o eliminado pools de almacenamiento en cloud?
- ¿Se han realizado cambios en la compresión o el cifrado del almacenamiento?
- ¿Se han producido cambios en la infraestructura de red? Por ejemplo, VLAN, enrutadores o DNS.
- ¿Se han realizado cambios en los orígenes de NTP?
- ¿Se han realizado cambios en las interfaces de red de cliente, administrador o grid?
- ¿Se han realizado otros cambios en el sistema StorageGRID o en su entorno?

Establecer líneas base

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

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

| Propiedad | Valor | Cómo obtener |
|--|-------------------------|---|
| Tasa de operaciones S3 | Operaciones por segundo | <p>En el panel de control de Grid Manager, seleccione Rendimiento > Operaciones S3 para nodos de almacenamiento.</p> <p>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.</p> |
| Tasa de evaluación de ILM | Objetos por segundo | <p>En la página Nodes, seleccione grid > ILM.</p> <p>En el gráfico de la cola de ILM, busque un período donde la línea sea bastante estable. Coloque el cursor sobre el gráfico para estimar un valor de línea base para Tasa de evaluación para su sistema.</p> |
| Tasa de análisis de ILM | Objetos por segundo | <p>Seleccione Nodos > grid > ILM.</p> <p>En el gráfico de la cola de ILM, busque un período donde la línea sea bastante estable. Coloque el cursor sobre el gráfico para estimar un valor de línea base para Tasa de exploración para su sistema.</p> |
| Objetos en cola de operaciones del cliente | Objetos por segundo | <p>Seleccione Nodos > grid > ILM.</p> <p>En el gráfico de la cola de ILM, busque un período donde la línea sea bastante estable. Coloque el cursor sobre el gráfico para estimar un valor de línea base para Objetos en cola (de operaciones del cliente) para su sistema.</p> |
| Latencia media de consultas | Milisegundos | <p>Seleccione Nodos > Nodo de almacenamiento > Objetos. En la tabla Consultas, vea el valor de Latencia promedio.</p> |

Análisis de datos

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

El análisis depende-problema, pero en general:

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

Lista de comprobación de información de escalado

Si no puede resolver el problema por su cuenta, póngase en contacto con el soporte técnico. Antes de

ponerse en contacto con el soporte técnico, recopile la información incluida en la siguiente tabla para facilitar la resolución del problema.

|  Elemento | Notas |
|--|---|
| Declaración de problema | <p>¿Cuáles son los síntomas del problema? ¿Cuándo comenzó el problema? ¿Ocurre de manera sistemática o intermitente? Si es intermitente, ¿qué veces ha ocurrido?</p> <p>Defina el problema</p> |
| Evaluación del impacto | <p>¿Cuál es la gravedad del problema? ¿Cómo afecta a la aplicación cliente?</p> <ul style="list-style-type: none"> • ¿Se ha conectado el cliente correctamente anteriormente? • ¿El cliente puede procesar, recuperar y eliminar datos? |
| ID del sistema StorageGRID | Seleccione Mantenimiento > Sistema > Licencia . El ID del sistema StorageGRID se muestra como parte de la licencia actual. |
| Versión de software | En la parte superior de Grid Manager, seleccione el ícono de ayuda y seleccione Acerca de para ver la versión de StorageGRID. |
| Personalización | <p>Resuma cómo se configura el sistema StorageGRID. Por ejemplo, enumere lo siguiente:</p> <ul style="list-style-type: none"> • ¿El grid utiliza compresión de almacenamiento, cifrado de almacenamiento o cumplimiento de normativas? • ¿Hace ILM objetos replicados o con código de borrado? ¿Garantiza ILM la redundancia de sitios? ¿Las reglas de ILM usan los comportamientos de ingestión de registro equilibrado, estricto o doble? |
| Registrar archivos y datos del sistema | <p>Recopile archivos de registro y datos del sistema para su sistema. Seleccione Soporte > Herramientas > Recopilación de registros.</p> <p>Es posible recopilar registros de toda la cuadrícula o de los nodos seleccionados.</p> <p>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 instalados en un sitio incluyen el servicio ADC.</p> |

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

Solucionar problemas de almacenamiento y objetos

Confirme las ubicaciones de los datos del objeto

En función del problema, es posible que desee hacerlo "[confirme dónde se almacenan los datos de objetos](#)". Por ejemplo, puede que desee verificar que la política de ILM esté funcionando como se espera y que los datos de objetos se almacenen donde estaba previsto.

Antes de empezar

- Debe tener un identificador de objeto, que puede ser uno de los siguientes:
 - **UUID:** Identificador único universal del objeto. Introduzca el UUID en todas las mayúsculas.
 - **CBID:** Identificador único del objeto dentro de StorageGRID . Es posible obtener el CBID de un objeto del registro de auditoría. Introduzca el CBID en todas las mayúsculas.
 - **S3 bucket y object key:** Cuando se ingiere un objeto a través de "[Interfaz de S3](#)", la aplicación cliente utiliza una combinación de bucket y object key 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 o una clave de objeto/depósito S3.

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

Object Metadata Lookup

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

Identifier

source/testobject

Version ID (optional)

MEJGMkMyQzgtNEY5OC0xMUU3LTkzMExlRDkyNTAwQkY5N0Mx

Look Up

4. Seleccione **Buscar**.

"resultados de consulta de metadatos de objetos" Aparece el. Esta página incluye los siguientes tipos de información:

- Metadatos del sistema, incluidos el ID de objeto (UUID), el ID de versión (opcional), el nombre del objeto, el nombre del contenedor, el nombre o el ID de la cuenta de inquilino, el tamaño lógico del objeto, la fecha y la hora en que se creó el objeto por primera vez, y la fecha y la hora en que se modificó por última vez el objeto.
- Todos los pares de valor de clave de metadatos de usuario personalizados asociados con el objeto.
- Para los objetos S3, cualquier par de etiqueta de objeto clave-valor asociado al objeto.
- Para las copias de objetos replicadas, la ubicación de almacenamiento actual de cada copia.
- Para las copias de objetos codificados de borrado, la ubicación actual de almacenamiento de cada fragmento.
- Para las copias de objetos en un Cloud Storage Pool, la ubicación del objeto, incluido el nombre del bloque externo y el identificador único del objeto.
- Para objetos segmentados y objetos multipartes, una lista de segmentos de objetos que incluyen identificadores de segmentos y tamaños de datos. Para objetos con más de 100 segmentos, sólo se muestran los primeros 100 segmentos.
- Todos los metadatos del objeto en el formato de almacenamiento interno sin procesar. Estos metadatos sin procesar incluyen los metadatos internos del sistema que no se garantiza que continúen del lanzamiento al lanzamiento.

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

System Metadata

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

Replicated Copies

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

Raw Metadata

Errores del almacén de objetos (volumen de almacenamiento)

El almacenamiento subyacente en un nodo de almacenamiento se divide en almacenes de objetos. Los almacenes de objetos también se conocen como volúmenes de almacenamiento.

Puede ver información del almacén de objetos para cada nodo de almacenamiento. Seleccione **Nodos > Nodo de almacenamiento > Almacenamiento**.

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 |

Dependiendo de la naturaleza del fallo, los fallos con un volumen de almacenamiento pueden reflejarse en "[alertas del volumen de almacenamiento](#)". Si un volumen de almacenamiento falla, debe reparar el volumen de almacenamiento con errores para restaurar el nodo de almacenamiento a Lo antes posible. con todas las funcionalidades. Si es necesario, puede ir a la pestaña **Configuración "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.

Verifique la integridad del objeto

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

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

¿Qué es la verificación en segundo plano?

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

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

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



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

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

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

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

Alertas relacionadas con la verificación en segundo plano

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

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

¿Qué es la comprobación de la existencia de objetos?

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

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

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

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

Ejecute la comprobación de existencia de objetos

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Usted tiene el "[Permiso de mantenimiento o acceso raíz](#)".
- 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 ejecutan en los nodos que desea comprobar:
 - La ampliación de grid para añadir un nodo de almacenamiento
 - Retirada del nodo de almacenamiento
 - Recuperación de un volumen de almacenamiento con fallos

- Recuperación de un nodo de almacenamiento con una unidad del sistema con errores
- Reequilibrio de EC
- Clon del nodo del dispositivo

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

Acerca de esta tarea

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

Pasos

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

Puede buscar por nombre de nodo o sitio.

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

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

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

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

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

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

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

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

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

- El trabajo finaliza.

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



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

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

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

Si 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.

11. Una vez completado el trabajo, realice las acciones necesarias adicionales:

- Si las copias de objeto que faltan detectadas son cero, no se encontraron problemas. No se requiere ninguna acción.
- Si la cantidad de copias de objetos faltantes detectadas es mayor que cero y no se ha activado la alerta **Objetos potencialmente perdidos**, el sistema reparó 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 potencialmente perdidos**, la integridad de los datos podría verse afectada. Póngase en contacto con el soporte técnico.
- Puede investigar copias de objetos potencialmente perdidas utilizando grep para extraer los mensajes de auditoría de LLST: `grep LLST audit_file_name`.

Este procedimiento es similar al de "[Investigando objetos potencialmente perdidos](#)" , aunque para las copias de objetos se busca LLST en lugar de OLST .

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

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

a. Seleccione **Mantenimiento > Comprobación de existencia de objetos > Historial de trabajos**.

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

- Observe la columna **tiempo final** para determinar qué trabajos se ejecutaron hace más de tres semanas.
- En el caso de estos trabajos, analice la columna de control de coherencia para obtener un sitio seguro o un entorno global sólido.

- c. Seleccione la casilla de verificación para cada trabajo que desee volver a ejecutar y, a continuación, seleccione **Volver a ejecutar**.
- d. En el asistente Rerun Jobs, revise los nodos y los volúmenes seleccionados y la coherencia.
- e. Cuando esté listo para volver a ejecutar los trabajos, seleccione **Rerun**.

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

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

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

Antes de empezar

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

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

Pasos

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

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

Al iniciar sesión como root, la petición de datos cambia de \$ a #.

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

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

| Opción | Destino |
|---------------------------------------|---|
| Nodos locales (predeterminado) | /var/local/log/localaudit.log |
| Nodos de administración/nodos locales | <ul style="list-style-type: none"> • Nodos de administración (principales y no principales): /var/local/audit/export/audit.log • Todos los nodos: El /var/local/log/localaudit.log archivo normalmente está vacío o falta en este modo. |
| Servidor de syslog externo | /var/local/log/localaudit.log |

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

Para obtener más información, consulte "[Seleccionar la ubicación del registro](#)".

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

- i. Introduzca zgrep SPUT * | egrep "CSIZ\ (UI64\):([5-9]\|[1-9]\ [0-9]\+)\ [0-9]\{9\}"
- ii. Para cada mensaje de auditoría en los resultados, consulte S3AI el campo para determinar el ID de cuenta de inquilino. Utilice los otros campos del mensaje para determinar la dirección IP utilizada por el cliente, el depósito y el objeto:

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

Ejemplo de resultados de registro de auditoría

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):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):PUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

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

- a. Vaya a **Soporte > Herramientas > Recopilación de registros**. Recopilar registros de aplicaciones para el nodo de almacenamiento en la alerta. Especifique 15 minutos antes y después de la alerta. Consulte "[Recopilar archivos de registro y datos del sistema](#)".
- b. Extraiga el archivo y vaya a bycast.log:

/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/broadcast.log

- c. Busque el log method=PUT e identifique al cliente en clientIP el campo.

Ejemplo bycast.log

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

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

Solucionar problemas de datos de objetos perdidos o faltantes

Solucionar problemas de datos de objetos perdidos o faltantes

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

El sistema StorageGRID utiliza 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 potencialmente perdidos**, de la siguiente manera:

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

Debe investigar todas las alertas de **Objetos potencialmente 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 potencialmente perdidos"](#)". Es posible que se activen falsas alertas de objetos perdidos como medida de precaución.

En el caso de que se pierdan datos de objetos sin copias, no existe solución de recuperación. Sin embargo, debes "["Restablecer el contador de objetos potencialmente perdidos"](#)" para evitar que los objetos perdidos conocidos enmascaren nuevos objetos perdidos.

Investigar objetos potencialmente perdidos

Cuando se activa la alerta **Objetos potencialmente 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 una "[navegador web compatible](#)".
- Tienes "[permisos de acceso específicos](#)".
- Debe tener el `Passwords.txt` archivo.

Acerca de esta tarea

La alerta **Objetos potencialmente perdidos** indica que, según la información disponible en StorageGRID, no hay copias de un objeto en la cuadrícula. Es posible que se hayan perdido datos de forma permanente.

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



Si se reporta la pérdida de más de 10 objetos, comuníquese con el soporte técnico. No siga este procedimiento usted mismo.

Pasos

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

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

4. Desde un nodo de administración, "[acceda al registro de auditoría](#)" para determinar el identificador único (UUID) del objeto que activó la alerta **Objetos potencialmente perdidos**:
 - a. Inicie sesión en el nodo de grid:
 - i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - iii. Introduzca el siguiente comando para cambiar a raíz: `su -`
 - iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo. Al iniciar sesión como root, la petición de datos cambia de `$` a `#`.
 - b. Cambie al directorio donde se encuentran los registros de auditoría.

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

| Opción | Destino |
|---------------------------------------|---|
| Nodos locales (predeterminado) | /var/local/log/localaudit.log |
| Nodos de administración/nodos locales | <ul style="list-style-type: none"> • Nodos de administración (principales y no principales): /var/local/audit/export/audit.log • Todos los nodos: El /var/local/log/localaudit.log archivo normalmente está vacío o falta en este modo. |

| Opción | Destino |
|----------------------------|-------------------------------|
| Servidor de syslog externo | /var/local/log/localaudit.log |

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

Para obtener más información, consulte "[Seleccionar la ubicación del registro](#)".

- c. Utilice grep para extraer los mensajes de auditoría de objetos perdidos (OLST). Introduzca: grep OLST audit_file_name
- d. Observe el valor de UUID incluido en el mensaje.

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

5. Busque los metadatos del objeto perdido mediante el UUID:

- a. Seleccione **ILM > Búsqueda de metadatos de objetos**.
- b. Ingresa el UUID y selecciona **Look Up**.
- c. Revise las ubicaciones de los metadatos y realice la acción correspondiente:

| Metadatos | Conclusión |
|--|--|
| <object_identifier> del objeto no encontrada | Si no se encuentra el objeto, se devuelve el mensaje "ERROR":". Si no se encuentra el objeto, Restablecer el contador de objetos potencialmente 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 potencialmente perdidos podría ser un falso positivo. Confirme que los objetos existen. Utilice el Id. De nodo y la ruta de archivo que aparecen en la salida para confirmar que el archivo de objeto está en la ubicación de la lista. Si los objetos existen, Restablecer el contador de objetos potencialmente perdidos para borrar la alerta. |

| Metadatos | Conclusión |
|-----------------|--|
| Ubicaciones = 0 | <p>Si no hay ubicaciones enumeradas en la salida, es posible que el objeto no esté presente. Póngase en contacto con el soporte técnico.</p> <p>Es posible que el soporte técnico le solicite determinar si hay un procedimiento de recuperación del almacenamiento en curso. Consulte la información "Restaurando datos de objetos con Grid Manager" sobre y. "restaurar datos de objeto en un volumen de almacenamiento"</p> |

6. Después de solucionar los problemas de objetos perdidos, restablezca el contador de Objetos potencialmente perdidos para asegurarse de que las alertas no sean falsos positivos:
 - a. Seleccionar **Nodos**.
 - b. Seleccione **Nodo de almacenamiento > Tareas**.
 - c. En la sección Restablecer contador de objetos potencialmente perdidos, seleccione **Restablecer**.

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

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

Antes de empezar

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

Acerca de esta tarea

La alerta **Low object data storage** se activa cuando la cantidad total de datos de objetos replicados y borrados en un nodo de almacenamiento cumple con una de las condiciones configuradas en la regla de alerta.

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

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

En esta condición:

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

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

Pasos

1. Seleccione **Alertas > Actual**.

Aparece la página Alertas.

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



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

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

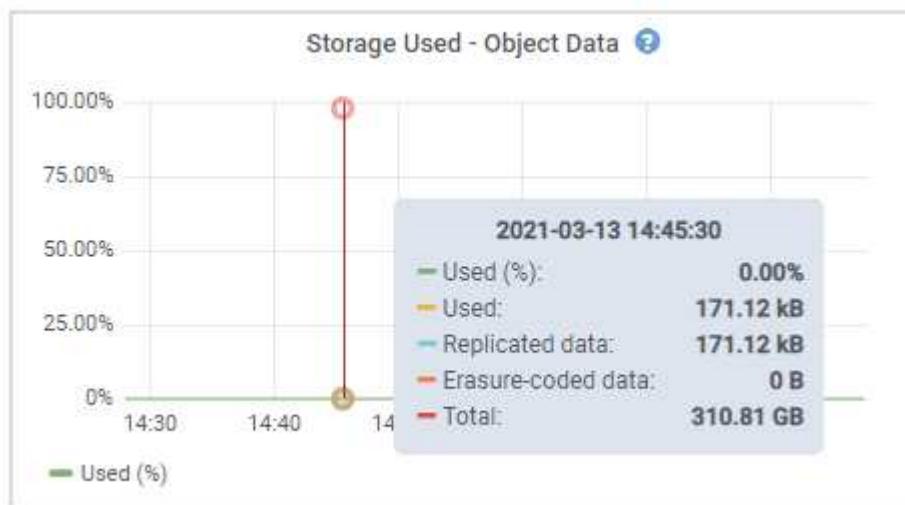
- Tiempo activado
- El nombre del sitio y del nodo
- Los valores actuales de las métricas de esta alerta

4. Seleccione **Nodos > Nodo de almacenamiento o Sitio > Almacenamiento**.

5. Coloque el cursor sobre el gráfico Almacenamiento Utilizado - Datos de Objeto.

Se muestran los siguientes valores:

- **Usado (%)**: El porcentaje del espacio útil total que se ha utilizado para datos de objeto.
- **Utilizado**: La cantidad de espacio útil total que se ha utilizado para los datos de objeto.
- **Datos replicados**: Estimación de la cantidad de datos de objetos replicados en este nodo, sitio o cuadrícula.
- **Datos codificados por borrado**: Estimación de la cantidad de datos de objetos codificados por borrado en este nodo, sitio o cuadrícula.
- **Total**: La cantidad total de espacio utilizable en este nodo, sitio o cuadrícula. El valor utilizado es `storagegrid_storage_utilization_data_bytes` la métrica.



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

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

7. Tan pronto como sea posible, "añadir capacidad de almacenamiento" a su red.

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



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

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

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

En versiones anteriores, los tres "[marcas de agua de volumen de almacenamiento](#)" eran la configuración global — los mismos valores se aplicaron a todos los volúmenes de almacenamiento en cada nodo de almacenamiento. A partir de StorageGRID 11.6, el software puede optimizar estas marcas de agua para cada volumen de almacenamiento en función del tamaño del nodo de almacenamiento y la capacidad relativa del volumen.

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

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

Comprenda la alerta

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

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

Por ejemplo, supongamos que previamente estableció la marca de agua de sólo lectura variable 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 | 12GB |
| Volumen 1 | 12GB |

| | |
|-----------|------|
| Volumen 2 | 11GB |
| Volumen 3 | 15GB |

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

Resolver la alerta

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

Antes de empezar

- Ha completado la actualización a StorageGRID 11.6 o superior.
- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Usted tiene el "[Permiso de acceso raíz](#)".

Acerca de esta tarea

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

Evalúe el uso de datos de objetos en todo el grid

Pasos

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

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 lleno (por ejemplo, todos los valores de **datos de objeto utilizados** son inferiores al 80%), puede empezar a utilizar la configuración de anulación. Vaya a [Utilice marcas de agua optimizadas](#).
- Si las reglas de ILM utilizan un comportamiento de procesamiento estricto o si los pools de almacenamiento específicos están casi completos, realice los pasos de [Vea las marcas de agua de almacenamiento optimizadas](#) y [Determine si puede utilizar marcas de agua optimizadas](#).

Ver marcas de agua de almacenamiento optimizadas

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

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 blanda de sólo lectura recomendada, introduzca la siguiente métrica Prometheus y seleccione **Ejecutar**:

```
storagegrid_storage_volume_minimum_optimized_soft_READONLY_watermark
```

La última columna muestra el valor mínimo optimizado de la marca de agua soft de solo lectura 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 **Baja anulación de marca de agua de solo lectura** para el nodo de almacenamiento.

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

```
storagegrid_storage_volume_maximum_optimized_soft_READONLY_watermark
```

La última columna muestra el valor máximo optimizado de la marca de agua soft read-only para todos los volúmenes de almacenamiento en cada nodo de almacenamiento.

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

Determine si puede utilizar marcas de agua optimizadas

Pasos

1. Seleccionar **Nodos**.
2. Repita estos pasos para cada nodo de almacenamiento en línea:
 - a. Seleccione **Storage Node > Storage**.
 - b. Desplácese hasta la tabla almacenes de objetos.
 - c. Compare el valor **disponible** de cada almacén de objetos (volumen) con la Marca de agua optimizada máxima que anotó para ese nodo de almacenamiento.
3. Si al menos un volumen 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 usar las marcas de agua optimizadas.

De lo contrario, amplíe la cuadrícula lo antes posible. ["añadir volúmenes de almacenamiento"](#) En un nodo existente o ["Añada nuevos nodos de almacenamiento"](#) en . A continuación, vaya a [Utilice marcas de agua optimizadas](#) para actualizar la configuración de las marcas de agua.

4. Si necesita continuar utilizando valores personalizados para las marcas de agua del volumen de almacenamiento, ["silencio"](#) o ["desactivar"](#) la alerta **Baja anulación de marca de agua de solo lectura**.



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

Utilice marcas de agua optimizadas

Pasos

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

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

volumen.

Solucionar problemas de metadatos

Si se producen problemas de metadatos, las alertas le informarán del origen de los problemas y las acciones recomendadas que debe realizar. En particular, debe añadir nuevos nodos de almacenamiento si se activa la alerta de almacenamiento de metadatos bajo.

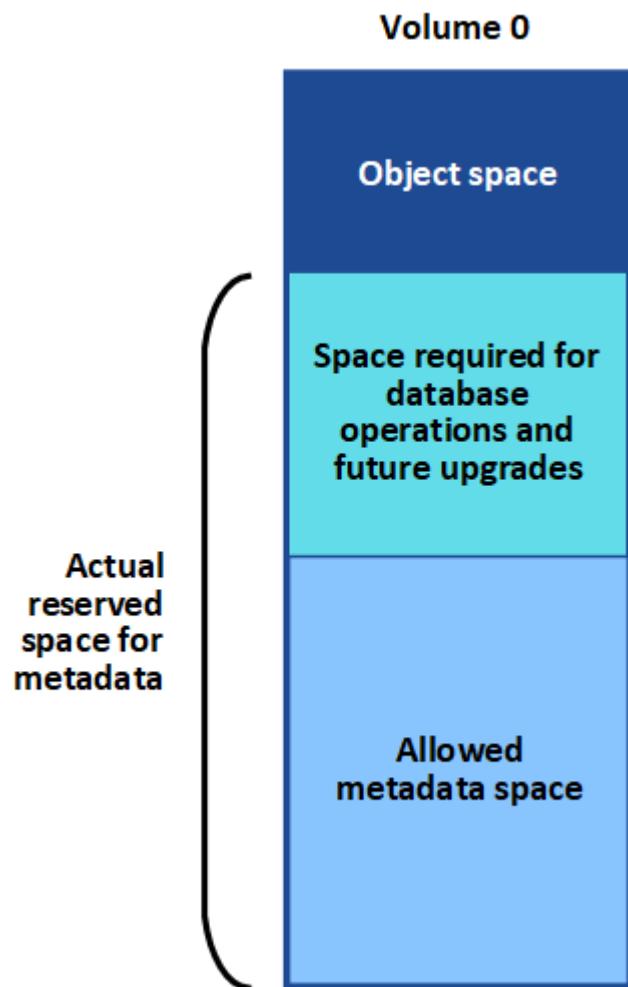
Antes de empezar

Ha iniciado sesión en Grid Manager mediante una "[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 del objeto. Este espacio, conocido como *espacio reservado real*, se subdivide en el espacio permitido para los metadatos del objeto (el espacio de metadatos permitido) y el espacio necesario para las operaciones esenciales de la base de datos, como la compactación y la reparación. El espacio de metadatos permitido rige la capacidad general del objeto.



Si los metadatos de objetos consumen más del 100% del espacio permitido para los metadatos, las

operaciones de la base de datos no se podrán ejecutar de manera eficiente y se producirán errores.

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

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

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza  
tion_metadata_allowed_bytes
```

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

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



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

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



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

Pasos

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



Dado que StorageGRID mantiene copias completas de todos los metadatos de objetos en cada sitio, la capacidad de metadatos del grid completo está limitada por la capacidad de metadatos del sitio más pequeño. Si necesita añadir capacidad de metadatos a un sitio, también ["expanda cualquier otro sitio"](#) debe usar la misma cantidad de nodos de almacenamiento.

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

Solucionar errores de certificado

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

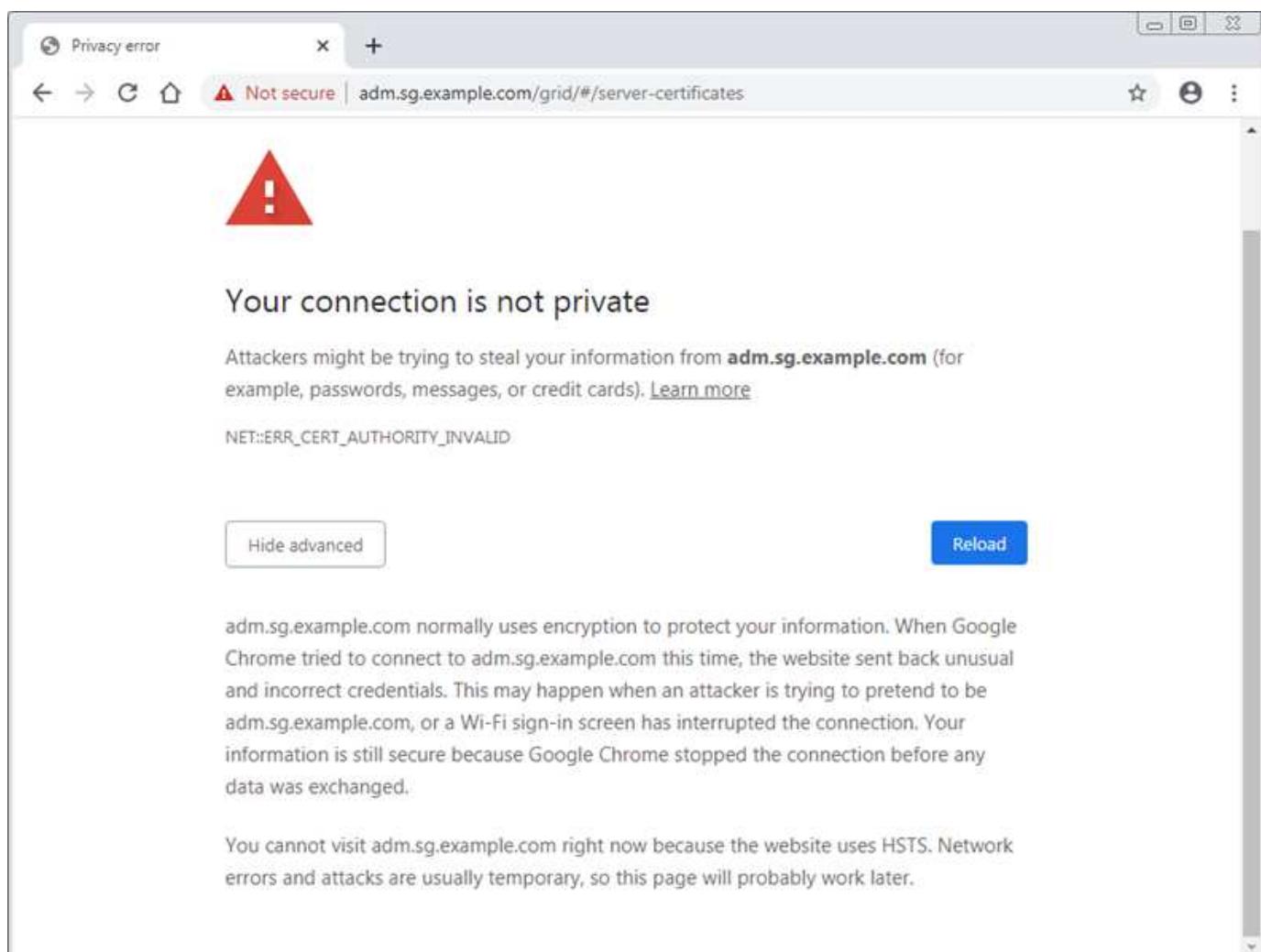
Acerca de esta tarea

Los errores de certificado pueden causar problemas al intentar conectarse a StorageGRID mediante el Administrador de grid, la API de gestión de grid, el Administrador de inquilinos o la API de gestión de inquilinos. Los errores de certificado también pueden ocurrir cuando intenta conectarse con un cliente S3 o una herramienta de monitoreo externa.

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

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

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



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

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

Pasos

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

1. Compruebe 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 caducado o lo hará pronto, cargue o genere uno nuevo.
 - Para obtener un certificado de servidor, consulte los pasos para "[Configuración de un certificado de servidor personalizado para el administrador de grid y el administrador de inquilinos](#)".
 - Para obtener un certificado de cliente, consulte los pasos para "[configurar un certificado de cliente](#)".
3. En el caso de errores de certificado de servidor, intente con una de las siguientes opciones o ambas:
 - Asegúrese de que se rellena el asunto Nombre alternativo (SAN) del certificado y que LA SAN coincida con la dirección IP o el nombre de host del nodo al que se conecta.
 - Si está intentando conectarse a StorageGRID con un nombre de dominio:
 - i. Introduzca la dirección IP del nodo de administración en lugar del nombre de dominio para omitir el error de conexión y acceder a Grid Manager.
 - ii. Desde el Administrador de red, seleccione **Configuración > Seguridad > Certificados** y luego "[seleccione la ficha de certificado adecuada](#)" para instalar un nuevo certificado personalizado o continuar con el certificado predeterminado.
 - iii. En las instrucciones para administrar StorageGRID, consulte los pasos para "[Configuración de un certificado de servidor personalizado para el administrador de grid y el administrador de inquilinos](#)".

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

Es posible ejecutar varias tareas para determinar el origen de los problemas relacionados con los nodos de administrador y la interfaz de usuario de StorageGRID.

Errores de inicio de sesión del nodo de administración

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante una "[navegador web compatible](#)".
- Tiene el `Passwords.txt` archivo.
- Tienes "[permisos de acceso específicos](#)".

Acerca de esta tarea

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

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

Pasos

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

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

2. Si su sistema StorageGRID tiene más de un nodo de administración, intente iniciar sesión en el Administrador de grid desde otro nodo de administración para comprobar 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. Determine si el hardware del nodo está sin conexión.

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



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

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

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

- Si el usuario local puede iniciar sesión:
 - i. Revisar las alertas.
 - ii. Seleccione **Configuración > Control de acceso > Federación de identidades**.
 - iii. Haga clic en **probar conexión** para validar la configuración de conexión para el servidor LDAP.
 - iv. Si la prueba falla, resuelva cualquier error de configuración.
- Si el usuario local no puede iniciar sesión y está seguro de que las credenciales son correctas, vaya al siguiente paso.

6. Utilice Secure Shell (SSH) para iniciar sesión en el nodo de administración:

- a. Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`

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

Al iniciar sesión como root, la petición de datos cambia de `$` a `#`.

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

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

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

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

- 8. Confirme que el servicio `nginx-gw` se está ejecutando `# service nginx-gw status`
- 9. Utilice Lumberjack para recopilar registros: `# /usr/local/sbin/lumberjack.rb`

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

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

10. Revise los siguientes registros:

- /var/local/log/bycast.log
- /var/local/log/bycast-err.log
- /var/local/log/nms.log
- **/*commands.txt

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

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

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

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

12. Desde el nodo de administración, utilice ssh para iniciar sesión en cada uno de los nodos de almacenamiento de ADC, utilizando las direcciones IP identificadas.
13. Vea el estado de todos los servicios que se ejecutan en el nodo de grid: storagegrid-status

Asegúrese de que los servicios idnt, acct, nginx y cassandra están en ejecución.

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

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

Problemas de la interfaz de usuario

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

Pasos

1. Asegúrese de que está utilizando una "[navegador web compatible](#)".
2. Borre la caché del navegador web.

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

instrucciones, consulte la documentación de su navegador web.

Solucionar problemas de red, hardware y plataforma

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

Errores de «422: Entidad no procesable»

El error 422: Entidad no procesable puede ocurrir por diferentes razones. Compruebe el mensaje de error para determinar la causa del problema.

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

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

| 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> | <p>Este mensaje aparece si intenta utilizar un cifrado no compatible para establecer una conexión TLS (Seguridad de la capa de transporte) desde StorageGRID a un sistema externo utilizado para identificar los grupos de almacenamiento de la federación o de la nube.</p> <p>Compruebe los códigos que ofrece el sistema externo. El sistema debe utilizar uno de los "Cifrados compatibles con StorageGRID" para las conexiones TLS salientes, como se muestra en las instrucciones para administrar StorageGRID.</p> |

Alerta de discrepancia de MTU de red de cuadrícula

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

Acerca de esta tarea

Las diferencias en la configuración de MTU podrían indicar que algunas redes eth0, pero no todas, están configuradas para tramas gigantes. Un error de coincidencia del tamaño de MTU de más de 1000 puede provocar problemas de rendimiento de la red.

Pasos

- El acceso SSH externo está bloqueado de forma predeterminada. Si es necesario, ["permitir el acceso temporalmente"](#).
- Enumere la configuración de MTU para eth0 en todos los nodos.
 - Utilice la consulta proporcionada en Grid Manager.
 - Navegue hasta `primary Admin Node IP address/metrics/graph` e introduzca la siguiente consulta: `node_network_mtu_bytes{device="eth0"}`
- ["Modifique la configuración de MTU"](#) Según sea necesario para garantizar que son iguales para la interfaz de red de grid (eth0) en todos los nodos.
 - Para nodos basados en Linux y VMware, use el siguiente comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

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

Nota: En los nodos basados en Linux, si el valor 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 tener el valor MTU deseado, y luego usar `change-ip.py` el script para cambiar el valor MTU de la red en el

contenedor.

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

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

+

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

4. Si ha permitido el acceso SSH externo, "[bloquear el acceso](#)" Cuando hayas terminado la tarea.

Alerta de error de trama de recepción de red de nodo

Las alertas de error de marco de recepción de red de nodos pueden deberse a problemas de conectividad entre StorageGRID y el hardware de la red. Esta alerta se borra por sí sola después de solucionar el problema subyacente.

Acerca de esta tarea

Las alertas de error de marco de recepción de red de nodos pueden deberse a los siguientes problemas con el hardware de red que se conecta a StorageGRID:

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

Pasos

1. Siga los pasos de solución de problemas para todas las causas potenciales de esta alerta en la configuración de red.
2. Realice los siguientes pasos en función de la causa del error:

FEC no coincide



Estos pasos solo se aplican a las alertas de error de marco de recepción de red de nodos* causadas por la discrepancia de FEC en los dispositivos StorageGRID.

- a. Compruebe el estado de FEC del puerto en el interruptor conectado al dispositivo StorageGRID.
- b. Compruebe la integridad física de los cables del aparato al interruptor.
- c. Si desea cambiar la configuración de FEC para intentar resolver la alerta, asegúrese primero de que el aparato está configurado para el modo **AUTO** en la página Configuración de enlace del instalador de dispositivos StorageGRID (consulte las instrucciones de su aparato):
 - ["SG6160"](#)
 - ["SGF6112"](#)
 - ["SG6000"](#)
 - ["SG5800"](#)
 - ["SG5700"](#)
 - ["SG110 y SG1100"](#)
 - ["SG100 y SG1000"](#)
- d. Cambie la configuración de FEC en los puertos del switch. Los puertos del dispositivo StorageGRID ajustarán los ajustes del FEC para que coincidan, si es posible.

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



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

Discrepancia entre el puerto del switch y la MTU de NIC

Si la alerta se debe a una discrepancia entre el puerto del switch y la MTU de NIC, compruebe que el tamaño de MTU configurado en el nodo sea igual que la configuración de MTU para el puerto del switch.

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



Para obtener el mejor rendimiento de red, todos los nodos deben configurarse con valores MTU similares en sus interfaces de Grid Network. La alerta **Red de cuadrícula MTU** se activa si hay una diferencia significativa en la configuración de MTU para la Red de cuadrícula en nodos individuales. No es necesario que los valores de MTU sean los mismos para todos los tipos de red. Consulte [Solucione problemas de la alerta de discrepancia de MTU de red de cuadrícula](#) para obtener más información.



Consulte también "[Cambio la configuración de MTU](#)".

Índices altos de errores de enlace

- a. Active FEC, si aún no está activado.
- b. Compruebe que el cableado de red es de buena calidad y que no está dañado o conectado incorrectamente.
- c. Si parece que los cables no son el problema, póngase en contacto con el soporte técnico.



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

Desbordamiento del búfer de anillo NIC

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

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

3. Supervise el problema y póngase en contacto con el soporte técnico si la alerta no se resuelve.

Errores de sincronización de hora

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

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



En el caso "[Especificación del origen NTP externo](#)" de una instalación de StorageGRID en el nivel de producción, no utilice el servicio Hora de Windows (W32Time) en una versión de Windows anterior a Windows Server 2016. El servicio de tiempo en versiones anteriores de Windows no es lo suficientemente preciso y no es compatible con Microsoft para su uso en entornos de gran precisión como StorageGRID.

Linux: Problemas de conectividad de red

Puede ver problemas con la conectividad de red de los nodos de StorageGRID alojados en hosts Linux.

Clonación de direcciones MAC

En algunos casos, los problemas de red se pueden resolver mediante la clonación de direcciones MAC. Si 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. Vea las instrucciones para "[crear archivos](#)

de configuración de nodo".



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

Para obtener más información, consulte las instrucciones para "[Habilitar la clonación de MAC](#)".

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 comutador virtual y grupo de puertos estén establecidas en **Aceptar** para el modo promiscuo, los cambios de dirección MAC y las transmisiones falsificadas. Los valores establecidos en el comutador virtual pueden ser anulados por los valores en el nivel de grupo de puertos, por lo que asegúrese de que la configuración sea la misma en ambos lugares.

Para obtener más información sobre el uso del modo promiscuo, consulte las instrucciones para "[Cómo configurar la red del host](#)".

Linux: El estado del nodo es «huérfano»

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

Acerca de esta tarea

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

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

Pasos

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

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

Si el nodo está huérfano, la respuesta es

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

4. Desde Linux, detenga el motor de contenedor y todos los procesos que controlan el nodo storagegrid. Por ejemplo:`sudo docker stop --time secondscontainer-name`

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

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

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

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

Linux: Solucione problemas de compatibilidad con IPv6

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

Acerca de esta tarea

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

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 de IPv6 en el kernel.

Pasos

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

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

El resultado debería ser 0.

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



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

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

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

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

El resultado debería ser 1.

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



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

5. Salga del contenedor: `exit`

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

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

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

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

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

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

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

Solucionar problemas de un servidor de syslog externo

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

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

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

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

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

- ["Consideraciones que tener en cuenta sobre el uso de un servidor de syslog externo"](#)
- ["Configurar la gestión de registros y el servidor syslog externo"](#)

| Mensaje de error | Descripción y acciones recomendadas |
|--|---|
| No se puede resolver el nombre de host | <p>El FQDN introducido para el servidor de syslog no se pudo resolver a una dirección IP.</p> <ol style="list-style-type: none">1. Compruebe el nombre de host que ha introducido. Si has introducido una dirección IP, asegúrate de que sea una dirección IP válida en una notación W.X.Y.Z («decimal con puntos»).2. Compruebe que los servidores DNS están configurados correctamente.3. Confirmar que cada nodo puede acceder a las direcciones IP del servidor DNS. |
| Conexión rechazada | <p>Se rechazó una conexión TCP o TLS con el servidor de syslog. Es posible que no haya escucha de servicio en el puerto TCP o TLS del host, o que un firewall esté bloqueando el acceso.</p> <ol style="list-style-type: none">1. Compruebe que haya introducido el FQDN o la dirección IP, el puerto y el protocolo correctos para el servidor de syslog.2. Confirme que el host para el servicio de syslog está ejecutando un daemon de syslog que se está escuchando en el puerto especificado.3. Confirme que un firewall no bloquea el acceso a las conexiones TCP/TLS desde los nodos a la IP y al puerto del servidor de syslog. |
| Red inaccesible | <p>El servidor de syslog no está en una subred de conexión directa. Un enrutador devolvió un mensaje de error ICMP para indicar que no pudo reenviar los mensajes de prueba de los nodos enumerados al servidor de syslog.</p> <ol style="list-style-type: none">1. Compruebe que haya introducido el FQDN o la dirección IP correctos para el servidor de syslog.2. Para cada nodo de la lista, compruebe la lista de subredes de redes de cuadrícula, las listas de subredes de redes de administración y las puertas de enlace de red de cliente. Confirmar que se han configurado para enrutar el tráfico al servidor de syslog a través de la interfaz de red y la puerta de enlace esperadas (Grid, Admin o Client). |

| Mensaje de error | Descripción y acciones recomendadas |
|--------------------------------------|--|
| Host inaccesible | <p>El servidor de syslog se encuentra en una subred de conexión directa (subred que utilizan los nodos mostrados para sus direcciones IP de grid, administrador o cliente). Los nodos intentaron enviar mensajes de prueba, pero no recibieron respuestas a las solicitudes ARP para la dirección MAC del servidor syslog.</p> <ol style="list-style-type: none"> 1. Compruebe que haya introducido el FQDN o la dirección IP correctos para el servidor de syslog. 2. Compruebe que el host que ejecuta el servicio de syslog esté configurado. |
| Tiempo de espera de conexión agotado | <p>Se ha realizado un intento de conexión TCP/TLS, pero no se ha recibido respuesta del servidor de syslog durante mucho tiempo. Es posible que haya una configuración incorrecta de enrutamiento o que un firewall esté borrando el tráfico sin enviar ninguna respuesta (una configuración común).</p> <ol style="list-style-type: none"> 1. Compruebe que haya introducido el FQDN o la dirección IP correctos para el servidor de syslog. 2. Para cada nodo de la lista, compruebe la lista de subredes de redes de cuadrícula, las listas de subredes de redes de administración y las puertas de enlace de red de cliente. Confirme que están configurados para enrutar el tráfico hacia el servidor de syslog mediante la interfaz de red y la puerta de enlace (Grid, Admin o Client) mediante las que espera acceder al servidor de syslog. 3. Confirme que un firewall no bloquea el acceso a las conexiones TCP/TLS desde los nodos indicados a la IP y al puerto del servidor de syslog. |
| Conexión cerrada por el partner | <p>Se estableció correctamente una conexión TCP con el servidor de syslog, pero se cerró posteriormente. Algunos motivos pueden ser:</p> <ul style="list-style-type: none"> • Es posible que se haya reiniciado o reiniciado el servidor de syslog. • Es posible que el nodo y el servidor de syslog tengan diferentes ajustes de TCP/TLS. • Un firewall intermedio podría estar cerrando conexiones TCP inactivas. • Es posible que un servidor que no esté escuchando en el puerto del servidor de syslog haya cerrado la conexión. <p>Para resolver este problema:</p> <ol style="list-style-type: none"> 1. Compruebe que haya introducido el FQDN o la dirección IP, el puerto y el protocolo correctos para el servidor de syslog. 2. Si utiliza TLS, confirme que el servidor de syslog también utiliza TLS. Si utiliza TCP, confirme que el servidor de syslog también utiliza TCP. 3. Compruebe que un firewall intermedio no está configurado para cerrar las conexiones TCP inactivas. |

| Mensaje de error | Descripción y acciones recomendadas |
|------------------------------------|--|
| Error del certificado de TLS | <p>El certificado de servidor recibido del servidor de syslog no era compatible con el paquete de certificado de CA y el certificado de cliente proporcionados.</p> <ol style="list-style-type: none"> Confirme que el paquete de certificado de CA y el certificado de cliente (si los hubiera) son compatibles con el certificado de servidor en el servidor de syslog. Confirme que las identidades en el certificado de servidor del servidor de syslog incluyen los valores esperados de IP o FQDN. |
| Reenvío suspendido | <p>Los registros de syslog ya no se reenvían al servidor de syslog y StorageGRID no puede detectar el motivo.</p> <p>Revise los registros de depuración proporcionados con este error para intentar determinar la causa raíz.</p> |
| Sesión TLS finalizada | <p>El servidor de syslog finalizó la sesión TLS y StorageGRID no puede detectar el motivo.</p> <ol style="list-style-type: none"> Revise los registros de depuración proporcionados con este error para intentar determinar la causa raíz. Compruebe que haya introducido el FQDN o la dirección IP, el puerto y el protocolo correctos para el servidor de syslog. Si utiliza TLS, confirme que el servidor de syslog también utiliza TLS. Si utiliza TCP, confirme que el servidor de syslog también utiliza TCP. Confirme que el paquete de certificado de CA y el certificado de cliente (si los hubiera) son compatibles con el certificado de servidor del servidor de syslog. Confirme que las identidades en el certificado de servidor del servidor de syslog incluyen los valores esperados de IP o FQDN. |
| Error en la consulta de resultados | <p>El nodo de administrador que se utiliza para la configuración y las pruebas del servidor de syslog no puede solicitar resultados de prueba a los nodos enumerados. Uno o más nodos pueden estar inactivos.</p> <ol style="list-style-type: none"> Siga los pasos estándar de solución de problemas para asegurarse de que los nodos estén en línea y que todos los servicios esperados estén en ejecución. Reinicie el servicio miscd en los nodos indicados. |

Solucionar problemas de almacenamiento en caché del balanceador de carga

Obtenga información sobre los posibles problemas con el almacenamiento en caché del equilibrador de carga y cómo solucionarlos.

Determinar si una solicitud fue un acierto de caché

- El encabezado X-Cache se establece en la respuesta a las solicitudes manejadas por el servicio de caché.
Códigos posibles:

- HIT: El objeto fue servido desde la caché
- PARTIAL-HIT: El depósito/clave tenía un registro en la memoria caché, pero no se pudo servir todo el rango solicitado desde la memoria caché.
- STALE: El depósito/clave tenía un registro en caché, pero el objeto se actualizó desde la última vez que se sirvió desde caché.
- MISS: El objeto no estaba en caché
- El nginx-gw/endpoint-access.log.gz El registro de la solicitud incluye "unix:/run/cache-svc/cache-svc.sock" para las solicitudes manejadas por la caché.
- El cache-svc/cache-svc.log informa un mensaje como, "Solicitud 320390: completada exitosamente (acceso a caché)" o "Solicitud 320375: completada exitosamente (error de caché)". Encuentre la ruta solicitada buscando otros registros con la misma cadena "Solicitud <número>".

Baja tasa de aciertos de caché

- Se pueden esperar tasas de aciertos de caché bajas cuando se agrega una nueva carga de trabajo o cuando cambia el conjunto de trabajo al que accede una carga de trabajo. En estas situaciones, se espera que la tasa de aciertos aumente con el tiempo.
- Si varias cargas de trabajo utilizan almacenamiento en caché, considere agregar políticas de clasificación de tráfico para aislar partes de las cargas de trabajo atendidas por el caché. Las métricas de tasa de aciertos de caché están disponibles según la política de clasificación de tráfico. Si algunas cargas de trabajo no experimentan buenas tasas de aciertos de caché, considere mover esas cargas de trabajo a otros puntos finales que no tengan el almacenamiento en caché habilitado.
- Evaluar la tasa de desalojo de caché. Si el caché es demasiado pequeño para adaptarse al conjunto de trabajo, experimentará altas tasas de desalojo y podría contribuir a tasas de aciertos más bajas.
- Es posible que haya opciones disponibles en FPVR para mejorar las tasas de acierto de ciertas cargas de trabajo.

Bajo rendimiento

- Evaluar la tasa de aciertos de caché. Las bajas tasas de aciertos de caché pueden generar un bajo rendimiento general.
- Evaluar la tasa de desalojo de caché. Durante el desalojo, se utilizan algunos recursos de almacenamiento para eliminar objetos existentes del disco. Si el proceso de desalojo no se mantiene al día con el acceso de nuevos objetos, el sistema puede alcanzar los umbrales de marca de agua y comenzar a omitir el caché.
- Verifique los límites de la red mediante los diagnósticos “Uso de recepción de interfaces de red” y “Uso de transmisión de interfaces de red”.

Revisar los registros de auditoría

Registros y mensajes de auditoría

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

Estas instrucciones son para los administradores responsables de generar informes sobre la actividad y el uso

del sistema que requieran analizar los mensajes de auditoría del sistema StorageGRID.

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

Para obtener información sobre cómo configurar los niveles de mensajes de auditoría y utilizar un servidor syslog externo, consulte "[Configurar la gestión de registros y el servidor syslog externo](#)" .

Auditar el flujo y la retención de mensajes

Todos los servicios de StorageGRID generan mensajes de auditoría durante el funcionamiento normal del sistema. Debe comprender el modo en que estos mensajes de auditoría se mueven al archivo a través del sistema StorageGRID audit.log.

Los siguientes flujos de trabajo para mensajes de auditoría y retención de mensajes de auditoría solo son aplicables si StorageGRID está configurado para **Nodos de administración/nodos locales** o **Nodo de administración y servidor syslog externo**. Si StorageGRID está configurado para "Solo nodos locales" (predeterminado) o "Servidor syslog externo", los mensajes de auditoría se guardan localmente en cada nodo del sistema. /var/local/log/localaudit.log archivo y no puede ser procesado por nodos de administración o nodos de almacenamiento.

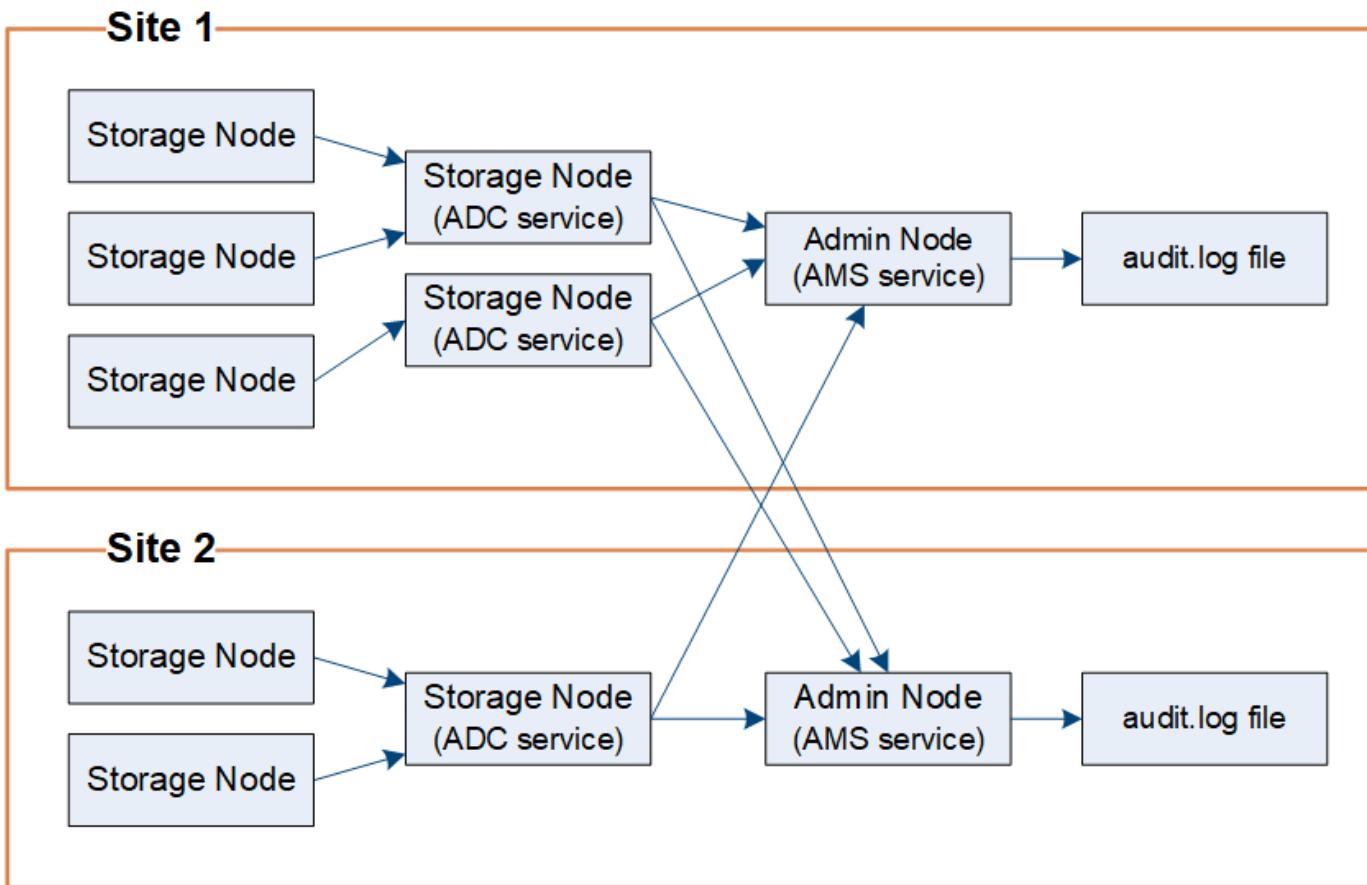
Flujo de mensajes de auditoría

Los mensajes de auditoría son procesados por los nodos de administración cuando StorageGRID está configurado para **Nodos de administración/nodos locales** o **Nodo de administración y servidor syslog externo** y por aquellos nodos de almacenamiento que tienen un servicio de controlador de dominio administrativo (ADC).

Como se muestra en el diagrama de flujo de mensajes de auditoría, cada nodo StorageGRID envía sus mensajes de auditoría a uno de los servicios ADC del sitio del centro de datos. El servicio ADC se habilita automáticamente para los primeros tres nodos de almacenamiento instalados en cada sitio.

A su vez, cada servicio ADC actúa como relé y envía su colección de mensajes de auditoría a cada nodo de administración del sistema StorageGRID, lo que proporciona a cada nodo de administración un registro completo de la actividad del sistema.

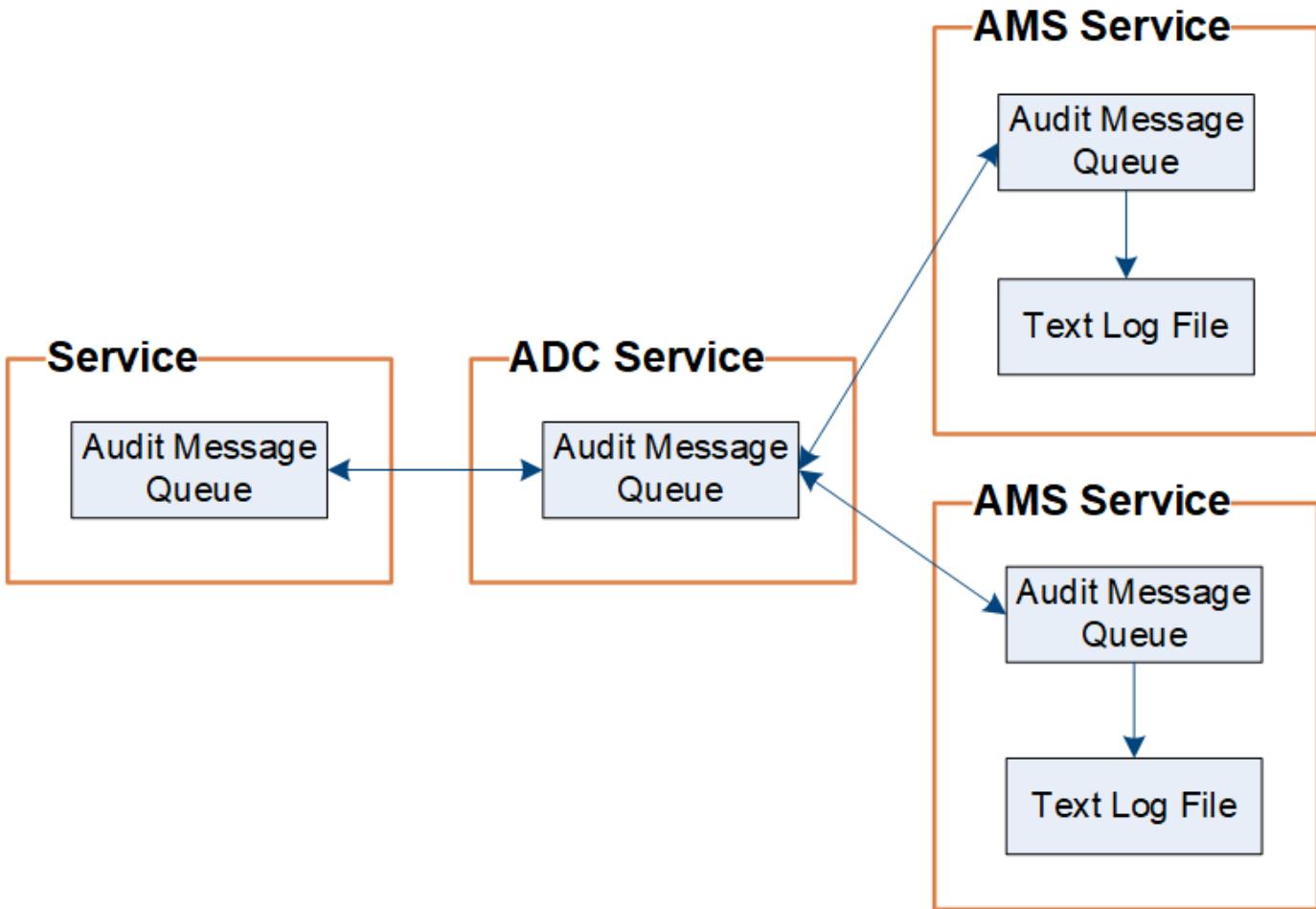
Cada nodo de administración almacena los mensajes de auditoría en archivos de registro de texto; el archivo de registro activo se denomina audit.log.



Retención de mensajes de auditoría

StorageGRID utiliza un proceso de copia y eliminación para garantizar que no se pierdan mensajes de auditoría antes de que puedan escribirse en el registro de auditoría.

Cuando un nodo genera o retransmite un mensaje de auditoría, el mensaje se almacena en una cola de mensajes de auditoría en el disco del sistema del nodo de la red. Siempre se guarda una copia del mensaje en una cola de mensajes de auditoría hasta que el mensaje se escribe en el archivo de registro de auditoría en el nodo de administración. `/var/local/audit/export` directorio. Esto ayuda a evitar la pérdida de un mensaje de auditoría durante el transporte.



La cola de mensajes de auditoría puede aumentar temporalmente debido a problemas de conectividad de red o capacidad de auditoría insuficiente. A medida que aumentan las colas, consumen más espacio disponible en cada nodo. /var/local/ directorio. Si el problema persiste y el directorio de mensajes de auditoría de un nodo se llena demasiado, los nodos individuales priorizan el procesamiento de su trabajo atrasado y dejan de estar disponibles temporalmente para recibir nuevos mensajes.

Especificamente, puede ver los siguientes comportamientos:

- Si el /var/local/audit/export Cuando el directorio utilizado por un nodo de administración se llena, dicho nodo se marca como no disponible para nuevos mensajes de auditoría hasta que el directorio ya no esté lleno. Las solicitudes de cliente S3 no se ven afectadas. La alarma XAMS (Repositorios de auditoría inaccesibles) se activa cuando un repositorio de auditoría no está disponible.
- Si el /var/local/ Cuando el directorio utilizado por un nodo de almacenamiento con el servicio ADC se llena en un 92 %, el nodo se marca como no disponible para auditar mensajes hasta que el directorio esté solo en un 87 % lleno. Las solicitudes del cliente S3 a otros nodos no se ven afectadas. La alarma NRY (Relés de auditoría disponibles) se activa cuando los relés de auditoría no están disponibles.



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

- Si el /var/local/ Cuando el directorio utilizado por un nodo de almacenamiento se llena al 85 %, el nodo comienza a rechazar solicitudes de clientes S3 con 503 Service Unavailable.

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

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

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

Para ayudarle a supervisar el tamaño de las colas de mensajes de auditoría a lo largo del tiempo, la alerta **cola de auditoría grande** y la alarma AMQS heredada se activan cuando el número de mensajes en una cola de nodos de almacenamiento o cola de nodos de administración alcanza determinados umbrales.

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

Si la alerta o alarma persiste y aumenta en gravedad, vea un gráfico del tamaño de la cola. Si el número aumenta de manera constante a lo largo de horas o días, es probable que la carga de auditoría haya excedido la capacidad de auditoría del sistema. Reduzca la tasa de operación del cliente o disminuya la cantidad de mensajes de auditoría registrados cambiando el nivel de auditoría de Escrituras de cliente y Lecturas de cliente a Error o Desactivado. Ver "["Configurar la gestión de registros y el servidor syslog externo"](#)" .

Mensajes duplicados

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

Acceda al archivo de registro de auditoría

El recurso compartido de auditoría contiene el archivo activo `audit.log` y los archivos de registro de auditoría comprimidos. Puede acceder a los archivos log de auditoría directamente desde la línea de comandos del nodo de administración.

El `audit.log` El archivo permanece vacío a menos que configure StorageGRID para **Nodos de administración/nodos locales** o **Nodo de administración y servidor syslog externo**. Para obtener más información, consulte "["Seleccionar la ubicación del registro"](#)" .

Antes de empezar

- Tienes "[permisos de acceso específicos](#)".
- Debe tener el `Passwords.txt` archivo.
- Debe conocer la dirección IP de un nodo de administrador.

Pasos

1. Inicie sesión en un nodo de administrador:

- a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
- b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

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

Al iniciar sesión como root, la petición de datos cambia de \$ a #.

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

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

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

Rotación del archivo de registro de auditoría

Si StorageGRID está configurado para **Nodos de administración/nodos locales** o **Nodo de administración y servidor syslog externo**, los archivos de registros de auditoría se guardan en el nodo de administración. /var/local/audit/export/ directorio. Los archivos de registro de auditoría activos se denominan audit.log .



Opcionalmente, puede cambiar el destino de los registros de auditoría y enviar información de auditoría a un servidor syslog externo. Los registros locales de registros de auditoría continúan generándose y almacenándose cuando se configura un servidor syslog externo. Consulte "["Configure los mensajes de auditoría y el servidor de syslog externo"](#)" .

Una vez al día, el archivo activo audit.log se guarda y se inicia un nuevo audit.log archivo. El nombre del archivo guardado indica cuándo se guardó, en el formato yyyy-mm-dd.txt. Si se crea más de un registro de auditoría en un solo día, los nombres de los archivos usan la fecha en que se guardó el archivo, anexado por un número, en el formato yyyy-mm-dd.txt.n. Por ejemplo, 2018-04-15.txt y 2018-04-15.txt.1 son los primeros y segundos archivos de registro creados y guardados el 15 de abril de 2018.

Después de un día, el archivo guardado se comprime y se renombra, en el formato yyyy-mm-dd.txt.gz , que conserva la fecha original. Con el tiempo, el almacenamiento del nodo de administración asignado para los registros de auditoría se consume. Un script monitorea el consumo de espacio del registro de auditoría y elimina archivos de registro según sea necesario para liberar espacio en el /var/local/audit/export/ directorio. Los registros de auditoría se eliminan según la fecha en que se crearon. Los registros más antiguos se eliminan primero. Puedes monitorizar las acciones del script en el siguiente archivo:

/var/local/log/manage-audit.log .

Este ejemplo muestra el archivo activo audit.log, el archivo del día anterior (2018-04-15.txt) y el archivo comprimido del día anterior (2018-04-14.txt.gz).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Formato del archivo de registro de auditoría

Formato del archivo de registro de auditoría

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

Cada mensaje de auditoría contiene lo siguiente:

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

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

- El mensaje de auditoría en sí, encerrado entre corchetes y empezando por AUDT.

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

2019-08-07T18:43:30.247711

```
[AUDT:[RSLT(FC32):SUFS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI  
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNT-  
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547  
18:root"]  
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc  
ket1"] [AVER(UI32):10] [ATIM(UI64):1565203410247711]  
[ATYP(FC32):PUT] [ANID(UI32):12454421] [AMID(FC32):S3RQ] [ATID(UI64):7074142  
142472611085]]
```

2019-08-07T18:43:30.783597

```
[AUDT:[RSLT(FC32):SUFS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA  
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNT-  
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547  
18:root"]  
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc  
ket1"] [S3KY(CSTR):"fh-small-0"]  
[CBID(UI64):0x779557A069B2C037] [UUID(CSTR):"94BA6949-38E1-4B0C-BC80-  
EB44FB4FCC7F"] [CSIZ(UI64):1024] [AVER(UI32):10]  
[ATIM(UI64):1565203410783597] [ATYP(FC32):PUT] [ANID(UI32):12454421] [AMID(F  
C32):S3RQ] [ATID(UI64):8439606722108456022]]
```

2019-08-07T18:43:30.784558

```
[AUDT:[RSLT(FC32):SUFS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA  
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]  
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNT-  
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547  
18:root"]  
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc  
ket1"] [S3KY(CSTR):"fh-small-2000"]  
[CBID(UI64):0x180CBD8E678EED17] [UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-  
E578D66F7ADD"] [CSIZ(UI64):1024] [AVER(UI32):10]  
[ATIM(UI64):1565203410784558] [ATYP(FC32):PUT] [ANID(UI32):12454421] [AMID(F  
C32):S3RQ] [ATID(UI64):13489590586043706682]]
```

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

Utilice la herramienta de explicación de auditoría

Puede usar `audit-explain` la herramienta para traducir los mensajes de auditoría del

registro de auditoría a un formato de fácil lectura.

Antes de empezar

- Tienes "[permisos de acceso específicos](#)".
- Debe tener el `Passwords.txt` archivo.
- Debe conocer la dirección IP del nodo de administrador principal.

Acerca de esta tarea

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

 `audit-explain`` La herramienta está destinada principalmente al soporte técnico durante las operaciones de solución de problemas. El procesamiento de ``audit-explain`` consultas puede consumir una gran cantidad de energía de CPU, lo que podría afectar a las operaciones de StorageGRID.

En este ejemplo se muestra la salida típica de `audit-explain` la herramienta. Estos cuatro ["SPUT"](#) mensajes de auditoría se generaron cuando el inquilino S3 con el ID de cuenta 92484777680322627870 utilizó S3 solicitudes PUT para crear un bloque llamado «bucket1» y añadir tres objetos a ese bloque.

```
PUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
PUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
PUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
PUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

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

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

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

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

- Procese varios archivos simultáneamente. Por ejemplo:

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

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

- Acepte la entrada de una tubería, lo que le permite filtrar y preprocesar la entrada mediante el grep

comando u otros medios. Por ejemplo:

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

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

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

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

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

Utilice la `help (-h)` opción para ver las opciones disponibles. Por ejemplo:

```
$ audit-explain -h
```

Pasos

1. Inicie sesión en el nodo de administración principal:

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

Al iniciar sesión como root, la petición de datos cambia de `$` a `#`.

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

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

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



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

Utilice la herramienta de suma de auditoría

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

Antes de empezar

- Tienes "permisos de acceso específicos".
- Tiene el Passwords.txt archivo.
- Conoce la dirección IP del nodo de administración principal.

Acerca de esta tarea

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

 audit-sum`La herramienta está destinada principalmente al soporte técnico durante las operaciones de solución de problemas. El procesamiento de `audit-sum consultas puede consumir una gran cantidad de energía de CPU, lo que podría afectar a las operaciones de StorageGRID.

En este ejemplo se muestra la salida típica de audit-sum la herramienta. Este ejemplo muestra el tiempo que tardaban las operaciones de protocolo.

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

El audit-sum La herramienta proporciona recuentos y tiempos para los siguientes mensajes de auditoría de S3 e ILM en un registro de auditoría.

 Los códigos de auditoría se eliminan del producto y de la documentación a medida que las funciones quedan obsoletas. Si encuentra un código de auditoría que no aparece aquí, consulte las versiones anteriores de este tema para ver versiones anteriores de StorageGRID . Por ejemplo, "["StorageGRID 11.8 Uso de la herramienta de suma de auditoría"](#) .

| Codificación | Descripción | Consulte |
|--------------|--|---|
| IDEL | ILM Initiated Delete: Registra cuando ILM inicia el proceso de eliminación de un objeto. | " IDEL: Eliminación de ILM iniciada " |
| SDEL | S3 DELETE: Registra una transacción realizada correctamente para eliminar un objeto o bloque. | " SDEL: ELIMINACIÓN DE S3 " |
| SGET | S3 GET: Registra una transacción realizada correctamente para recuperar un objeto o enumerar los objetos de un bloque. | " SGET: S3 GET " |
| SHEA | S3 HEAD: Registra una transacción realizada correctamente para comprobar la existencia de un objeto o bloque. | " SHEA: CABEZA S3 " |
| SPUT | S3 PUT: Registra una transacción realizada correctamente para crear un nuevo objeto o bloque. | " SPUT: S3 PUT " |

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

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

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

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

- Procese varios archivos simultáneamente. Por ejemplo:

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

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

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

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```

Esta herramienta no acepta archivos comprimidos como entrada canalizada. Para procesar archivos comprimidos, proporcione sus nombres de archivo como argumentos de línea de comando o utilice el zcat herramienta para descomprimir los archivos primero. Por ejemplo:

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

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



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

Utilice la `help (-h)` opción para ver las opciones disponibles. Por ejemplo:

```
$ audit-sum -h
```

Pasos

1. Inicie sesión en el nodo de administración principal:

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

Al iniciar sesión como root, la petición de datos cambia de `$` a `#`.

2. Si desea analizar todos los mensajes relacionados con las operaciones de escritura, lectura, cabeza y eliminación, siga estos pasos:

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

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

En este ejemplo se muestra la salida típica de `audit-sum` la herramienta. Este ejemplo muestra el tiempo que tardaban las operaciones de protocolo.

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

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

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

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

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

```
Total:          201906 operations
Slowest:        1740.290 sec
Average:        1.132 sec
Fastest:        0.010 sec
Slowest operations:
  time(usec)      source ip      type      size(B)  path
  ======  ======  ======  ======  =====
  1740289662    10.96.101.125  object    5663711385
backup/r901OaQ8JB-1566861764-4519.iso
  1624414429    10.96.101.125  object    5375001556
backup/r901OaQ8JB-1566861764-6618.iso
  1533143793    10.96.101.125  object    5183661466
backup/r901OaQ8JB-1566861764-4518.iso
  70839         10.96.101.125  object    28338
bucket3/dat.1566861764-6619
  68487         10.96.101.125  object    27890
bucket3/dat.1566861764-6615
  67798         10.96.101.125  object    27671
bucket5/dat.1566861764-6617
  67027         10.96.101.125  object    27230
bucket5/dat.1566861764-4517
  60922         10.96.101.125  object    26118
bucket3/dat.1566861764-4520
  35588         10.96.101.125  object    11311
bucket3/dat.1566861764-6616
  23897         10.96.101.125  object    10692
bucket3/dat.1566861764-4516
```

+

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

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

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

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

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

4. Si quieres determinar si las recuperaciones eran lentas ayer:

- a. Emite el comando en el registro de auditoría adecuado y utilice la opción group-by-time (-gt), seguido del período de tiempo (por ejemplo, 15M, 1H, 10S):

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

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

Estos resultados muestran que el tráfico GET de S3 aumentó entre las 06:00 y las 07:00. Los tiempos máximos y promedio son considerablemente más altos durante este lapso de tiempo y no aumentaron gradualmente a medida que aumentaba el recuento. Estas métricas sugieren que se excedió la capacidad, posiblemente en la red o en la capacidad de la red para procesar solicitudes.

- b. Para determinar qué objetos de tamaño se recuperaban ayer cada hora, agregue la opción size (-s) al comando:

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

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

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

- c. Para ver más detalles, utilice "[herramienta audit-explain](#)" para revisar todas las operaciones de SGET durante esa hora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Si se espera que la salida del comando grep sea muchas líneas, agregue el less comando para mostrar el contenido del archivo log de auditoría una página (una pantalla) a la vez.

- 5. Si desea determinar si las operaciones SPUT en los segmentos son más lentas que las operaciones SPUT para los objetos:

- a. Comience por usar -go la opción, que agrupa los mensajes para las operaciones de objeto y bloque por separado:

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

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

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

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

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

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

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

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

| message group | count | min (B) | max (B) |
|-----------------------------------|---------|---------|----------|
| average (B) | | | |
| ===== | ===== | ===== | ===== |
| SPUT.cho-non-versioning 21.672 | 71943 | 2.097 | 5000.000 |
| SPUT.cho-versioning 21.120 | 54277 | 2.097 | 5000.000 |
| SPUT.cho-west-region 14.433 | 80615 | 2.097 | 800.000 |
| SPUT.1dt002 0.352 | 1564563 | 0.000 | 999.972 |

Formato de mensaje de auditoría

Formato de mensaje de auditoría

Los mensajes de auditoría intercambiados dentro del sistema StorageGRID incluyen información estándar común a todos los mensajes y contenido específico que describe el evento o la actividad que se está reportando.

Si la información de resumen proporcionada por "[auditoría-explicar](#)" las herramientas y "[suma de auditoría](#)" no es suficiente, consulte esta sección para comprender el formato general de todos los mensajes de auditoría.

El siguiente es un mensaje de auditoría de ejemplo que puede aparecer en el archivo de registro de auditoría:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

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

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

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

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

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

En la siguiente lista se describen los elementos del atributo:

- ATTR es un código de cuatro caracteres para el atributo que se informa. Hay algunos atributos que son comunes a todos los mensajes de auditoría y a otros que son específicos de eventos.
- type Es un identificador de cuatro caracteres del tipo de datos de programación del valor, como UI64, FC32, etc. El tipo está entre paréntesis ().
- value es el contenido del atributo, normalmente un valor numérico o de texto. Los valores siempre siguen a dos puntos (:). Los valores del tipo de dato CSTR están rodeados por comillas dobles.

Tipos de datos

Se utilizan diferentes tipos de datos para almacenar información en mensajes de auditoría.

| Tipo | Descripción |
|------|--|
| UI32 | Entero largo sin signo (32 bits); puede almacenar los números de 0 a 4,294,967,295. |
| UI64 | Entero doble largo sin signo (64 bits); puede almacenar los números de 0 a 18,446,744,073,709,551,615. |
| FC32 | Constante de cuatro caracteres; un valor entero sin signo de 32 bits representado como cuatro caracteres ASCII como ABCD. |
| IPAD | Se usa para direcciones IP. |
| CSTR | Matriz de longitud variable de caracteres UTF-8. Los caracteres se pueden escapar con las siguientes convenciones: <ul style="list-style-type: none">• La barra invertida es \.• El retorno del carro es \r.• Las comillas dobles son \".• La alimentación de línea (nueva línea) es \n.• Los caracteres se pueden sustituir por sus equivalentes hexadecimales (en el formato \xHH, donde HH es el valor hexadecimal que representa el carácter). |

Datos específicos de un evento

Cada mensaje de auditoría del registro de auditoría registra datos específicos de un evento del sistema.

Después del contenedor de apertura [AUDT: que identifica el mensaje en sí, el siguiente juego de atributos proporciona información sobre el evento o la acción descrita por el mensaje de auditoría. Estos atributos se resaltan en el siguiente ejemplo:

```

2018-12-SUST08:24:45.921845 [AUDT:*|[RSLT\FC32]:SUCS]* *|[TIME\UI64]:11454
60025621595611246499[SUST08\SAIP\IPAD]:"10.224.0 60025621595611246499.100
60025621595611246499"\[S3AI\ECSTR]:"CSTR\\\"[CSTR]\[CSTR]\\\"[CSTR][CSTR]\\\"[CSTR][
CSTR][CSTR]\\\"[CSTR][CSTR]\[CSTR]\\\"[CSTR][CSTR]\[CSTR][CSTR]\\\"[CSTR][CSTR]\\\"[CSTR][
CSTR]\\\"[CSTR][CSTR]\\\"[CSTR]\\\"[KJC][KJC]\\"
15552417629170647261 12281045 1543998285921845 10 30720

```

`ATYP` El elemento (subrayado en el ejemplo) identifica qué evento generó el mensaje. Este mensaje de ejemplo incluye `xref:{relative_path}shea-s3-head.html["SHEA"]` el código de mensaje ([ATYP(FC32):SHEA]), que indica que se generó mediante una solicitud de S3 HEAD correcta.

Elementos comunes de los mensajes de auditoría

Todos los mensajes de auditoría contienen los elementos comunes.

| Codificación | Tipo | Descripción |
|--------------|------|--|
| EN MEDIO | FC32 | ID del módulo: Identificador de cuatro caracteres del ID del módulo que generó el mensaje. Indica el segmento de código en el que se generó el mensaje de auditoría. |
| ANID | UI32 | Node ID: El ID del nodo de grid asignado al servicio que generó el mensaje. A cada servicio se le asigna un identificador único en el momento en que se configura e instala el sistema StorageGRID. Este ID no se puede cambiar. |
| ASES | UI64 | Identificador de sesión de auditoría: En versiones anteriores, este elemento indicó la hora a la que se inicializó el sistema de auditoría después de que se iniciara el servicio. Este valor de tiempo se midió en microsegundos desde la época del sistema operativo (00:00:00 UTC el 1 de enero de 1970). Nota: este elemento es obsoleto y ya no aparece en los mensajes de auditoría. |
| ASQN | UI64 | Recuento de secuencias: En versiones anteriores, este contador se ha incrementado para cada mensaje de auditoría generado en el nodo de cuadrícula (ANID) y se ha restablecido a cero en el reinicio del servicio. Nota: este elemento es obsoleto y ya no aparece en los mensajes de auditoría. |
| AID | UI64 | ID de seguimiento: Identificador que comparte el conjunto de mensajes activados por un solo evento. |

| Codificación | Tipo | Descripción |
|------------------------|------|--|
| ATIM | UI64 | <p>Marca de hora: Hora en la que se generó el evento que activó el mensaje de auditoría, medida en microsegundos desde la época del sistema operativo (00:00:00 UTC el 1 de enero de 1970). Tenga en cuenta que la mayoría de las herramientas disponibles para convertir la Marca de tiempo a fecha y hora local se basan en milisegundos.</p> <p>Es posible que sea necesario redondear o truncar la Marca de tiempo registrada. El tiempo legible por el usuario que aparece al principio del mensaje de auditoría en el audit.log archivo es el atributo ATIM en formato ISO 8601. La fecha y la hora se representan <code>YYYY-MM-DDTHH:MM:SS.UUUUUU</code> como , donde el T es un carácter de cadena literal que indica el comienzo del segmento de tiempo de la fecha. UUUUUU son microsegundos.</p> |
| ATYP | FC32 | Tipo de evento: Identificador de cuatro caracteres del evento que se está registrando. Esto rige el contenido de "carga útil" del mensaje: Los atributos que se incluyen. |
| PROTECTOR | UI32 | Versión: Versión del mensaje de auditoría. A medida que el software StorageGRID evoluciona, las nuevas versiones de los servicios podrían incorporar nuevas funciones en los informes de auditorías. Este campo permite la compatibilidad con versiones anteriores del servicio AMS para procesar mensajes de versiones anteriores de servicios. |
| TRANSFORMACIÓN DIGITAL | FC32 | Resultado: Resultado del evento, proceso o transacción. Si no es relevante para un mensaje, NO SE utiliza NINGUNO en lugar de SUCS para que el mensaje no se filtre accidentalmente. |

Ejemplos de mensajes de auditoría

Puede encontrar información detallada en cada mensaje de auditoría. Todos los mensajes de auditoría tienen el mismo formato.

A continuación se muestra un mensaje de auditoría de ejemplo, tal y como podría aparecer en audit.log el archivo:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):PUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

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

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

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

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

El siguiente mensaje de auditoría también muestra el bloque al que está asociado el objeto:

```
2014-07-17T21:17:58.959669
[AUDT: [RSLT(FC32) :SUCS] [TIME(UI64) :246979] [S3AI(CSTR) :"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR) :"UJXDKKQOXB7YARDS71Q2"] [S3BK\ (CSTR\ ) :s3small11] [S3
KY(CSTR) :"hello1"] [CBID(UI64) :0x50C4F7AC2BC8EDF7] [CSIZ(UI64) :
0] [AVER(UI32) :10] [ATIM(UI64) :1405631878959669] [ATYP(FC32) :SPU
T] [ANID(UI32) :12872812] [AMID(FC32) :S3RQ] [ATID(UI64) :15792241
4102530435]]
```

Para detectar cuándo se produjo el evento PUT, anote la Marca de hora de hora universal coordinada (UTC) al comienzo del mensaje de auditoría. Este valor es una versión legible por humanos del atributo ATIM del mensaje de auditoría en sí:

```
2014-07-17T21:17:58.959669
[AUDT: [RSLT(FC32) :SUCS] [TIME(UI64) :246979] [S3AI(CSTR) :"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR) :"UJXDKKQOXB7YARDS71Q2"] [S3BK(CSTR) :"s3small11"] [S3K
Y(CSTR) :"hello1"] [CBID(UI64) :0x50C4F7AC2BC8EDF7] [CSIZ(UI64) :0
] [AVER(UI32) :10] [ATIM\ (UI64\ ) :1405631878959669] [ATYP(FC32) :SP
UT] [ANID(UI32) :12872812] [AMID(FC32) :S3RQ] [ATID(UI64) :15792241
44102530435]]
```

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

Auditar los mensajes y el ciclo de vida del objeto

¿Cuándo se generan los mensajes de auditoría?

Se generan mensajes de auditoría cada vez que se procesa, recupera o elimina un objeto. Puede identificar estas transacciones en el registro de auditoría ubicando los mensajes de auditoría específicos de S3 API.

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

| Protocolo | Codificación |
|---|---|
| Vinculación de operaciones de S3 | S3BK (cuchara), S3KY (llave) o ambos |
| Vinculación de las operaciones internas | CBID (identificador interno del objeto) |

Plazos de los mensajes de auditoría

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

Transacciones de procesamiento de objetos

Puede identificar las transacciones de ingestión de clientes en el registro de auditoría mediante la ubicación de S3 mensajes de auditoría específicos de la API.

No todos los mensajes de auditoría generados durante una transacción de ingestión aparecen en la siguiente tabla. Solo se incluyen los mensajes necesarios para rastrear la transacción de ingestión.

Mensajes de auditoría de incorporación de S3

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

Ejemplo: Ingesta de objetos S3

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

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



En el ejemplo siguiente no se enumeran todos los mensajes de auditoría generados durante una transacción. Solo se muestran los relacionados con la transacción de procesamiento de S3 (S3PUT).

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

S3PUT: S3 PUT

El mensaje SPUT se genera para indicar que se ha emitido una transacción PUT de S3 para crear un objeto en un segmento específico.

2017-07-

```
17T21:17:58.959669 [AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10.96.112.29"] [S3AI(CSTR):"70899244468554783528"] [SACC(CSTR):"test"] [S3AK(CSTR):"SGKHyalRU_5cLflqajtaFmxJn9461AWRJfBF33gAOg=="] [SUSR(CSTR):"urn:sgws:identity::70899244468554783528:root"] [SBAI(CSTR):"70899244468554783528"] [S3AC(CSTR):"test"] [S3BK(CSTR):"example"] [S3KY(CSTR):"testobject-0-3"] [CBID\ (UI64\):0x8EF52DF8025E63A8] [CSIZ(UI64):30720] [AVER(UI32):10] [ATIM(UI64):150032627859669] [ATYP\ (FC32\):PUT] [ANID(UI32):12086324] [AMID(FC32):S3RQ] [ATID(UI64):14399932238768197038]]
```

ORLM: Se cumplen las reglas de objeto

El mensaje ORLM indica que la política ILM se ha cumplido con este objeto. El mensaje incluye el CBID del objeto y el nombre de la regla ILM que se aplicó.

Para los objetos replicados, el campo LOCS incluye el ID de nodo LDR y el ID de volumen de las ubicaciones de objetos.

2019-07-

```
17T21:18:31.230669 [AUDT:[CBID\ (UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make 2 Copies"] [STAT(FC32):DONE] [CSIZ(UI64):0] [UUID(CSTR):"0B344E18-98ED-4F22-A6C8-A93ED68F8D3F"] [LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543 2147552014"] [RSLT(FC32):SUCS] [AVER(UI32):10] [ATYP\ (FC32\):ORLM] [ATIM(UI64):1563398230669] [ATID(UI64):15494889725796157557] [ANID(UI32):13100453] [AMID(FC32):BCMS]]
```

En el caso de los objetos con código de borrado, el campo LOCS incluye el identificador de perfil de código de borrado y el identificador de grupo de códigos de borrado

```
2019-02-23T01:52:54.647537
[AUDT: [CBID (UI64) :0xFA8ABE5B5001F7E2] [RULE (CSTR) :"EC_2_plus_1"] [STAT (FC32)
:DONE] [CSIZ (UI64) :10000] [UUID (CSTR) :"E291E456-D11A-4701-8F51-
D2F7CC9AFeca"] [LOCS (CSTR) :"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"] [RSLT (FC32) :SUCS] [AVER (UI32) :10] [ATIM (UI64) :1550929974537] \ [
ATYP\ (FC32\ ) :ORLM\ ] [ANID (UI32) :12355278] [AMID (FC32) :ILMX] [ATID (UI64) :41685
59046473725560]]
```

El campo PATH incluye información clave y del bucket S3.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT: [CBID (UI64) :0x82704DFA4C9674F4] [RULE (CSTR) :"Make 2
Copies"] [STAT (FC32) :DONE] [CSIZ (UI64) :3145729] [UUID (CSTR) :"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"] [PATH (CSTR) :"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"] [LOCS (CSTR) :"CLDI 12525468, CLDI
12222978"] [RSLT (FC32) :SUCS] [AVER (UI32) :10] [ATIM (UI64) :1568555574559] [ATYP (
FC32) :ORLM] [ANID (UI32) :12525468] [AMID (FC32) :OBDI] [ATID (UI64) :3448338865383
69336]]
```

Objeto: Eliminar transacciones

Puede identificar transacciones de supresión de objetos en el registro de auditoría ubicando mensajes de auditoría específicos de la API de S3.

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

S3 elimina mensajes de auditoría

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

Ejemplo: Eliminación de objetos de S3

Cuando un cliente S3 elimina un objeto de un nodo de almacenamiento (servicio LDR), se genera un mensaje de auditoría y se guarda en el registro de auditoría.



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

SDEL: Eliminación S3

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

2017-07-

```
17T21:17:58.959669 [AUDT: [RSLT (FC32) :SUCS] [TIME (UI64) :14316] [SAIP (IPAD) :"10  
.96.112.29"] [S3AI (CSTR) :"70899244468554783528"] [SACC (CSTR) :"test"] [S3AK (CS  
TR) :"SGKHyalRU_5cLf1qajtaFmxJn9461AWRJfBF33gA0g=="] [SUSR (CSTR) :"urn:sgws:i  
dentity::70899244468554783528:root"] [SBAI (CSTR) :"70899244468554783528"] [SB  
AC (CSTR) :"test"] \[S3BK\ (CSTR\ ) :"example"\] \[S3KY\ (CSTR\ ) :"testobject-0-  
7"\] [CBID\ (UI64\ ) :0x339F21C5A6964D89] [CSIZ (UI64) :30720] [AVER (UI32) :10] [ATI  
M (UI64) :150032627859669] [ATYP\ (FC32\ ) :SDEL] [ANID (UI32) :12086324] [AMID (FC32  
) :S3RQ] [ATID (UI64) :4727861330952970593]]
```

El objeto recupera las transacciones

Puede identificar las transacciones de recuperación de objetos en el registro de auditoría ubicando los mensajes de auditoría específicos de la API de S3.

No todos los mensajes de auditoría generados durante una transacción de recuperación aparecen en la siguiente tabla. Sólo se incluyen los mensajes necesarios para rastrear la transacción recuperada.

Mensajes de auditoría de recuperación de S3

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

Ejemplo: Recuperación de objetos de S3

Cuando un cliente S3 recupera un objeto de un nodo de almacenamiento (servicio LDR), se genera un mensaje de auditoría y se guarda en el registro de auditoría.

Tenga en cuenta que no todos los mensajes de auditoría generados durante una transacción se muestran en el siguiente ejemplo. Solo se muestran las relacionadas con la transacción de recuperación de S3 (SGET).

SGET: S3 GET

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

```
2017-09-20T22:53:08.782605
```

```
[AUDT:[RSLT(FC32):SUFS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-a"][S3AK(CSTR):"SGKht7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-O_Few=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-a"]\[S3BK\](CSTR):"bucket-anonymous"\]\[S3KY\](CSTR):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\](FC32):SGET\[ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
```

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

En el siguiente mensaje de ejemplo, el cliente envía una solicitud GetObject para un objeto almacenado en un depósito que no es de su propiedad. Los valores para SBAI y SBAC registran el ID y el nombre de la cuenta de inquilino del propietario del bloque, que difieren del ID de cuenta de inquilino y del nombre del cliente registrado en S3AI y SACC.

```
2017-09-20T22:53:15.876415
```

```
[AUDT:[RSLT(FC32):SUFS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI\](CSTR):"17915054115450519830"\]\[SACC\](CSTR):"s3-account-a"\][S3AK(CSTR):"SGKhpolW1P_kBkqSCbTi754Ls81BUog67I2L1SiUg=="][SUSR(CSTR):"urn:sgws:identity::17915054115450519830:root"]\[SBAI\](CSTR):"43979298178977966408"\]\[SBAC\](CSTR):"s3-account-a"\][S3BK(CSTR):"bucket-anonymous"]\[S3KY(CSTR):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Ejemplo: S3 Select en un objeto

Cuando un cliente S3 emite una consulta S3 Select en un objeto, se generan mensajes de auditoría y se guardan en el registro de auditoría.

Tenga en cuenta que no todos los mensajes de auditoría generados durante una transacción se muestran en el siguiente ejemplo. Solo se muestran los relacionados con la transacción Select de S3 (SelectObjectContent).

Cada consulta da como resultado dos mensajes de auditoría: Uno que realiza la autorización de la solicitud S3 Select (el campo S3SR está definido en "SELECT") y una OPERACIÓN GET posterior que recupera los datos del almacenamiento durante el procesamiento.

2021-11-08T15:35:30.750038

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI  
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten  
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id  
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA  
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-  
05064f74126d"][S3KY(CSTR):"SUB-  
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-  
9F01-4EE7-B133-  
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64)  
:1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]  
[ATID(UI64):1363009709396895985]]
```

2021-11-08T15:35:32.604886

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA  
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"\\"x-forwarded-  
for\":\\unix:\\}"] [S3AI(CSTR):"63147909414576125820"] [SACC(CSTR):"Tenant16  
36027116"] [S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"] [SUSR(CSTR):"urn:sgws:identit  
y::63147909414576125820:root"] [SBAI(CSTR):"63147909414576125820"] [SBAC(CST  
R):"Tenant1636027116"] [S3BK(CSTR):"619c0755-9e38-42e0-a614-  
05064f74126d"] [S3KY(CSTR):"SUB-  
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-  
9F01-4EE7-B133-  
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32)  
:10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A  
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Mensajes de actualización de metadatos

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

Mensajes de auditoría de actualización de metadatos S3

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

Ejemplo: Actualización de metadatos de S3

El ejemplo muestra una transacción correcta para actualizar los metadatos de un objeto S3 existente.

SUPD: Actualización de metadatos S3

El cliente S3 realiza una solicitud (SUPD) para actualizar los metadatos especificados(x-amz-meta-*) para el objeto S3 (S3KY). En este ejemplo, los encabezados de solicitud se incluyen en el campo HTRH porque se ha configurado como un encabezado de protocolo de auditoría (*Configuración* > **Monitoreo > Servidor de auditoría y syslog**). Ver "["Configurar la gestión de registros y el servidor syslog externo"](#)" .

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUFS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):{"\\"accept-encoding\\":\\"identity\\",\\"authorization\\":\\"AWS
LIUF17FGJARQHPY2E761:jul/hnzs/uNY+aVvV0lTSYhEGts=\\"",

\"content-length\\":\\"0\\",\\"date\\":\\"Tue, 11 Jul 2017 21:54:03
GMT\\",\\"host\\":\\"10.96.99.163:18082\\",
\"user-agent\\":\\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\\",
\"x-amz-copy-source\\":\\"/testbkt1/testobj1\\",\\"x-amz-metadata-
directive\\":\\"REPLACE\\",\\"x-amz-meta-city\\":\\"Vancouver\\"}]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Auditar mensajes

Descripciones de mensajes de auditoría

En las secciones siguientes se enumeran descripciones detalladas de los mensajes de auditoría devueltos por el sistema. Cada mensaje de auditoría aparece primero en una tabla que agrupa los mensajes relacionados por la clase de actividad que representa el mensaje. Estas agrupaciones son útiles tanto para comprender los tipos de actividades auditadas como para seleccionar el tipo deseado de filtrado de mensajes de auditoría.

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

Los códigos de cuatro caracteres utilizados en este capítulo son los valores ATYP que se encuentran en los mensajes de auditoría, como se muestra en el siguiente mensaje de ejemplo:

2014-07-17T03:50:47.484627

\ [AUDT: [RSLT(FC32):VRGN] [AVER(UI32):10] [ATIM(UI64):1405569047484627] [**ATYP\FC32\ :SYSU**] [ANID(UI32):11627225] [AMID(FC32):ARNI] [ATID(UI64):94457363265 00603516]]

Para obtener información sobre cómo configurar los niveles de mensajes de auditoría, cambiar los destinos de los registros y usar un servidor syslog externo para su información de auditoría, consulte "["Configurar la gestión de registros y el servidor syslog externo"](#)"

Auditar categorías de mensajes

Mensajes de auditoría del sistema

Los mensajes de auditoría que pertenecen a la categoría de auditoría del sistema se utilizan para eventos relacionados con el propio sistema de auditoría, los estados de los nodos de la cuadrícula, la actividad de tareas en todo el sistema (tareas de grid) y las operaciones de copia de seguridad de servicio.

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

| Codificación | Título del mensaje y descripción | Consulte |
|--------------|--|---|
| LLST | Ubicación perdida: Este mensaje de auditoría se genera cuando se pierde una ubicación. | " LLST: Ubicación perdida " |
| OLST | Objeto perdido: Un objeto solicitado no se puede ubicar dentro del sistema StorageGRID. | " OLST: El sistema detectó un objeto perdido " |
| AGREGAR | Deshabilitación de auditoría de seguridad: Se ha desactivado el registro de mensajes de auditoría. | " SADD: Desactivación de auditoría de seguridad " |
| SADE | Habilitación de auditoría de seguridad: Se ha restaurado el registro de mensajes de auditoría. | " SADE: Activación de auditoría de seguridad " |
| SRF | Error de verificación del almacén de objetos: Un bloque de contenido ha fallado las comprobaciones de verificación. | " SVRF: Fallo de verificación del almacén de objetos " |
| SVRU | Verificación de almacén de objetos desconocida: Se han detectado datos de objeto inesperados en el almacén de objetos. | " SVRU: Verificación del almacén de objetos desconocida " |
| SYSD | Node Stop: Se ha solicitado un apagado. | " SYSD: Parada del nodo " |
| SYST | Nodo de detención: Un servicio ha iniciado una detención elegante. | " SYST: Nodo detenido " |
| SYSU | Node Start: Se ha iniciado un servicio; la naturaleza del apagado anterior se indica en el mensaje. | " SYSU: Inicio del nodo " |

Mensajes de auditoría del almacenamiento de objetos

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



Los códigos de auditoría se eliminan del producto y de la documentación a medida que las funciones están obsoletas. Si encuentra un código de auditoría que no se muestra aquí, revise las versiones anteriores de este tema para ver versiones de SG anteriores. Por ejemplo, "["Mensajes de auditoría del almacenamiento de objetos de StorageGRID 11,8"](#)".

| Codificación | Descripción | Consulte |
|--------------|--|---|
| BROR | Solicitud de solo lectura de bloque: Un bloque entró o salió del modo de solo lectura. | " BROR: Solicitud de solo lectura de bucket " |

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

El cliente lee los mensajes de auditoría

Los mensajes de auditoría de lectura del cliente se registran cuando una aplicación cliente S3 realiza una solicitud para recuperar un objeto.

| Codificación | Descripción | Utilizado por | Consulte |
|--------------|--|---------------|--|
| S3SL | S3 Seleccionar solicitud: Registra una finalización después de que una solicitud de S3 Select se ha devuelto al cliente. El mensaje S3SL puede incluir detalles de mensaje de error y código de error. Es posible que la solicitud no se haya realizado correctamente. | Cliente S3 | " S3SL: S3 Seleccione la solicitud " |

| Codificación | Descripción | Utilizado por | Consulte |
|--------------|--|---------------|-------------------------------------|
| SGET | S3 GET: Registra una transacción realizada correctamente para recuperar un objeto o enumerar los objetos de un bloque. Nota: Si la transacción opera en un subrecurso, el mensaje de auditoría incluirá el campo S3SR. | Cliente S3 | " SGET: S3 GET " |
| SHEA | S3 HEAD: Registra una transacción realizada correctamente para comprobar la existencia de un objeto o bloque. | Cliente S3 | " SHEA: CABEZA S3 " |

El cliente escribe mensajes de auditoría

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

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

Mensaje de auditoría de gestión

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

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

Mensajes de auditoría de ILM

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

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

Referencia de mensajes de auditoría

BROR: Solicitud de solo lectura de bucket

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

| Codificación | Campo | Descripción |
|--------------|---|---|
| BKHD | UUID de bloque | El ID de bloque. |
| BROV | Valor de solicitud de sólo lectura del segmento | Si el depósito se está convirtiendo en de solo lectura o si está dejando el estado de solo lectura (1 = de solo lectura, 0 = no de solo lectura). |
| BROS | Motivo de sólo lectura del depósito | El motivo por el que el depósito se convierte en de sólo lectura o deja el estado de sólo lectura. Por ejemplo, emptyBucket. |
| S3AI | S3 ID de cuenta de inquilino | El ID de la cuenta de inquilino que envió la solicitud. Un valor vacío indica acceso anónimo. |
| S3BK | S3 cucharón | El nombre de bloque de S3. |

CBRB: Inicio de recepción de objetos

Durante las operaciones normales del sistema, los bloques de contenido se transfieren de forma continua entre diferentes nodos a medida que se accede a los datos, se replican y se conservan. Cuando se inicia la transferencia de un bloque de contenido de un nodo a otro, la entidad de destino emite este mensaje.

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

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

CBRE: Fin de recepción de objeto

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

| Codificación | Campo | Descripción |
|------------------------|---------------------------------------|---|
| CNID | Identificador de conexión | El identificador único de la sesión/conexión nodo a nodo. |
| CBID | Identificador de bloque de contenido | Identificador único del bloque de contenido que se está transfiriendo. |
| CTDR | Dirección de transferencia | Indica si la transferencia CBID se inició mediante inserción o se inició con extracción: INSERCIÓN: La entidad emisora solicitó la operación de transferencia. PULL: La entidad receptora solicitó la operación de transferencia. |
| CTSR | Entidad de origen | El ID de nodo de la fuente (remitente) de la transferencia CBID. |
| CTD | Entidad de destino | El ID de nodo del destino (receptor) de la transferencia CBID. |
| CTSS | Recuento de secuencias de inicio | Indica el recuento de secuencias en el que se inició la transferencia. |
| CTA | Recuento de secuencias finales reales | Indica que el último número de secuencias se ha transferido correctamente. Si el recuento de secuencia final real es el mismo que el recuento de secuencia de inicio y el resultado de la transferencia no se realizó correctamente, no se intercambiaron datos. |
| TRANSFORMACIÓN DIGITAL | Resultado de la transferencia | El resultado de la operación de transferencia (desde el punto de vista de la entidad emisora): SUCS: Transferencia finalizada correctamente; se enviaron todos los conteos de secuencia solicitados. CONL: Conexión perdida durante la transferencia CTMO: Tiempo de espera de la conexión durante el establecimiento o la transferencia UNRE: No se puede acceder al ID del nodo de destino CRPT: La transferencia finalizó debido a la recepción de datos corruptos o no válidos |

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

CBSB: Inicio de envío de objeto

Durante las operaciones normales del sistema, los bloques de contenido se transfieren de forma continua entre diferentes nodos a medida que se accede a los datos, se replican y se conservan. Cuando se inicia la transferencia de un bloque de contenido de un nodo a otro, la entidad de origen emite este mensaje.

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

Este mensaje de auditoría significa que se ha iniciado una operación de transferencia de datos nodo a nodo

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

CBSE: Fin de envío de objeto

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

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

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

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

CGRR: Solicitud de Replicación de Cuadrícula Cruzada

Este mensaje se genera cuando StorageGRID intenta realizar una operación de replicación entre grid para replicar objetos entre buckets de una conexión de federación de grid.

| Codificación | Campo | Descripción |
|--------------|--------------------------------------|---|
| CSIZ | Tamaño del objeto | <p>El tamaño del objeto en bytes.</p> <p>El atributo CSIZ se introdujo en StorageGRID 11,8. Como resultado, las solicitudes de replicación entre grid que abarcan una actualización de StorageGRID 11,7 a 11,8 podrían tener un tamaño de objeto total impreciso.</p> |
| S3AI | S3 ID de cuenta de inquilino | ID de la cuenta de inquilino propietaria del depósito desde el que se replica el objeto. |
| GFID | ID de conexión de federación de grid | El ID de la conexión de federación de grid que se utiliza para la replicación entre grid. |

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

EBDL: Eliminación de bloque vacío

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

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

EBKR: Solicitud de depósito vacío

Este mensaje indica que un usuario ha enviado una solicitud para activar o desactivar el depósito vacío (es decir, para suprimir objetos de depósito o para dejar de suprimir objetos).

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

ECMC: Falta el fragmento de datos con código de borrado

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

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

ECOC: Fragmento de datos con código de borrado corrupto

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

| Codificación | Campo | Descripción |
|------------------------|-----------------|---|
| VCCO | ID DEL VCS | El nombre del VCS que contiene el fragmento dañado. |
| VLID | ID del volumen | El volumen RangeDB que contiene el fragmento con código de borrado dañado. |
| CCID | ID de fragmento | El identificador del fragmento codificado por borrado dañado. |
| TRANSFORMACIÓN DIGITAL | Resultado | Este campo tiene el valor 'NONE'. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje en particular. 'NINGUNO' se utiliza en lugar de 'UCS' para que este mensaje no se filtre. |

ETAF: Error de autenticación de seguridad

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

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

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

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

GNRG: Registro GNDS

El servicio CMN genera este mensaje de auditoría cuando un servicio ha actualizado o registrado información sobre sí mismo en el sistema StorageGRID.

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

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

GNUR: Registro de GNDS

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

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

GTED: La tarea de la red terminó

Este mensaje de auditoría indica que el servicio CMN ha terminado de procesar la tarea de cuadrícula especificada y ha movido la tarea a la tabla histórica. Si el resultado es SUCS, ABRT o ROLF, habrá un mensaje de auditoría iniciado tarea de cuadrícula correspondiente. Los otros resultados indican que el procesamiento de esta tarea de cuadrícula nunca se ha iniciado.

| Codificación | Campo | Descripción |
|------------------------|----------------|--|
| TSID | ID de la tarea | <p>Este campo identifica de forma única una tarea de cuadrícula generada y permite gestionar la tarea de cuadrícula a lo largo de su ciclo de vida.</p> <p>Nota: el Id. De tarea se asigna en el momento en que se genera una tarea de cuadrícula, no en el momento en que se envía. Es posible que una tarea de cuadrícula determinada se envíe varias veces y, en este caso, el campo Id. De tarea no es suficiente para vincular de forma única los mensajes de auditoría enviados, iniciados y terminados.</p> |
| TRANSFORMACIÓN DIGITAL | Resultado | <p>El resultado final del estado de la tarea de la cuadrícula:</p> <ul style="list-style-type: none"> • SUCS: La tarea de la red se completó correctamente. • ABRT: La tarea de cuadrícula ha finalizado sin un error de rollback. • ROLF: La tarea de cuadrícula ha finalizado y no ha podido completar el proceso de rollback. • CANC: La tarea de cuadrícula fue cancelada por el usuario antes de iniciarse. • EXPR: La tarea de la cuadrícula ha caducado antes de iniciarse. • IVLD: La tarea de la cuadrícula no era válida. • AUTH: La tarea de la cuadrícula no estaba autorizada. • DUPL: La tarea de la cuadrícula se rechazó como duplicado. |

GTST: Se ha iniciado la tarea de cuadrícula

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

| Codificación | Campo | Descripción |
|------------------------|----------------|---|
| TSID | ID de la tarea | <p>Este campo identifica de forma única una tarea de cuadrícula generada y permite gestionar la tarea a lo largo de su ciclo de vida.</p> <p>Nota: el Id. De tarea se asigna en el momento en que se genera una tarea de cuadrícula, no en el momento en que se envía. Es posible que una tarea de cuadrícula determinada se envíe varias veces y, en este caso, el campo Id. De tarea no es suficiente para vincular de forma única los mensajes de auditoría enviados, iniciados y terminados.</p> |
| TRANSFORMACIÓN DIGITAL | Resultado | <p>El resultado. Este campo solo tiene un valor:</p> <ul style="list-style-type: none"> • SUCS: La tarea de red se inició correctamente. |

GTSU: Se ha enviado la tarea de la cuadrícula

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

| Codificación | Campo | Descripción |
|------------------------|------------------------------------|---|
| TSID | ID de la tarea | Identifica de forma única una tarea de cuadrícula generada y permite gestionar la tarea a lo largo de su ciclo de vida. Nota: el Id. De tarea se asigna en el momento en que se genera una tarea de cuadrícula, no en el momento en que se envía. Es posible que una tarea de cuadrícula determinada se envíe varias veces y, en este caso, el campo Id. De tarea no es suficiente para vincular de forma única los mensajes de auditoría enviados, iniciados y terminados. |
| TTYP | Tipo de tarea | Tipo de tarea de cuadrícula. |
| TVER | Versión de la tarea | Número que indica la versión de la tarea de cuadrícula. |
| TDSC | Descripción de la tarea | Una descripción legible por el usuario de la tarea de cuadrícula. |
| VATS | Válido después de la Marca de hora | El primer momento (UINT64 microsegundos a partir del 1 de enero de 1970 - tiempo UNIX) en el que es válida la tarea de la cuadrícula. |
| VBTS | Válido antes de la Marca de hora | La última hora (UINT64 microsegundos a partir del 1 de enero de 1970 - tiempo UNIX) en la que es válida la tarea de la cuadrícula. |
| TSRC | Origen | El origen de la tarea: <ul style="list-style-type: none">• TXTB: La tarea de la cuadrícula se envió a través del sistema StorageGRID como un bloque de texto firmado.• CUADRÍCULA: La tarea de la cuadrícula se envió a través del servicio interno de envío de tareas de la cuadrícula. |
| ACTV | Tipo de activación | Tipo de activación: <ul style="list-style-type: none">• AUTO: La tarea de cuadrícula se envió para la activación automática.• PEND: La tarea de cuadrícula se ha enviado a la tabla pendiente. Esta es la única posibilidad para la fuente TXTB. |
| TRANSFORMACIÓN DIGITAL | Resultado | El resultado de la presentación: <ul style="list-style-type: none">• SUCS: La tarea de la red se envió correctamente.• ERROR: La tarea se ha movido directamente a la tabla histórica. |

IDEL: Eliminación de ILM iniciada

Este mensaje se genera cuando ILM inicia el proceso de eliminación de un objeto.

El mensaje IDEL se genera en cualquiera de estas situaciones:

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

| Codificación | Campo | Descripción |
|--------------|---|--|
| CBID | Identificador de bloque de contenido | El CBID del objeto. |
| CMPA | Cumplimiento: Eliminación automática | Para objetos solo en bloques de S3 que cumplen con la normativa. 0 (falso) o 1 (verdadero), que indica si un objeto compatible debe eliminarse automáticamente cuando finalice su período de retención, a menos que el segmento se encuentre bajo una retención legal. |
| CMPL | Cumplimiento: Conservación legal | Para objetos solo en bloques de S3 que cumplen con la normativa. 0 (falso) o 1 (verdadero), que indica si el cubo está actualmente bajo un derecho. |
| CMPR | Cumplimiento: Período de retención | Para objetos solo en bloques de S3 que cumplen con la normativa. La duración del período de retención del objeto en minutos. |
| CTME | Cumplimiento de normativas: Tiempo de consumo | Para objetos solo en bloques de S3 que cumplen con la normativa. Tiempo de procesamiento del objeto. Puede agregar el período de retención en minutos a este valor para determinar cuándo se puede eliminar el objeto del bloque. |
| DMRK | Eliminar ID de versión del marcador | El código de versión del marcador de borrado creado al eliminar un objeto de un bloque con versiones. Las operaciones en los depósitos no incluyen este campo. |
| CSIZ | Tamaño de contenido | El tamaño del objeto en bytes. |

| Codificación | Campo | Descripción |
|------------------------|-------------------------------|---|
| BLOQUEOS | Ubicaciones | <p>La ubicación de almacenamiento de los datos del objeto dentro del sistema StorageGRID. El valor para LOCS es "" si el objeto no tiene ubicaciones (por ejemplo, se ha eliminado).</p> <p>CLEC: Para los objetos con código de borrado, el ID de perfil de codificación de borrado y el ID de grupo de codificación de borrado que se aplica a los datos del objeto.</p> <p>CLDI: Para los objetos replicados, el ID de nodo LDR y el ID de volumen de la ubicación del objeto.</p> <p>CLNL: ID de nodo DE ARCO de la ubicación del objeto si se archivan los datos del objeto.</p> |
| RUTA | S3 Cubo/llave | El nombre del cubo S3 y el nombre de la clave S3. |
| TRANSFORMACIÓN DIGITAL | Resultado | <p>Resultado de la operación de ILM.</p> <p>SUCS: La operación de ILM fue exitosa.</p> |
| REGLA | Etiqueta de reglas | <ul style="list-style-type: none"> Si un objeto de un bloque de S3 compatible se elimina automáticamente debido a que su período de retención ha caducado, este campo está en blanco. Si el objeto se está eliminando porque no hay más instrucciones de ubicación que se apliquen actualmente al objeto, este campo muestra la etiqueta legible para seres humanos de la última regla de ILM que se aplicó al objeto. |
| SGRP | Planta (grupo) | Si está presente, el objeto se eliminó en el sitio especificado, que no es el sitio donde se ingirió el objeto. |
| UUID | Identificador único universal | El identificador del objeto dentro del sistema StorageGRID. |
| VSID | ID de versión | El código de versión de la versión específica de un objeto que se eliminó. Las operaciones en cubos y objetos en depósitos sin versiones no incluyen este campo. |

LKCU: Limpieza de objetos sobreescritos

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

| Codificación | Campo | Descripción |
|--------------|-------------------------------|---|
| CSIZ | Tamaño de contenido | El tamaño del objeto en bytes. |
| LLEYP | Tipo de limpieza | <i>Uso interno solamente.</i> |
| LUID | UUID de objeto eliminado | Identificador del objeto que se ha eliminado. |
| RUTA | S3 Cubo/llave | El nombre del cubo S3 y el nombre de la clave S3. |
| SEGC | UUID del contenedor | UUID del contenedor del objeto segmentado. Este valor sólo está disponible si el objeto está segmentado. |
| UUID | Identificador único universal | Identificador del objeto que sigue existiendo. Este valor sólo está disponible si el objeto no se ha eliminado. |

LKDM: Limpieza de objetos filtrados

Este mensaje se genera cuando se limpia o elimina un fragmento filtrado. Un fragmento puede formar parte de un objeto replicado o de un objeto codificado con borrado.

| Codificación | Campo | Descripción |
|--------------|------------------------|---|
| CLOC | Ubicación del segmento | Ruta de acceso del archivo del fragmento filtrado que se ha eliminado. |
| CTYP | Tipo de segmento | Tipo de fragmento: ec: Erasure-coded object chunk repl: Replicated object chunk |

| Codificación | Campo | Descripción |
|--------------|--------------------------------------|--|
| LLEYP | Tipo de fuga | <p>Los cinco tipos de fugas que se pueden detectar:</p> <p>object_leaked: Object doesn't exist in the grid</p> <p>location_leaked: Object exists in the grid, but found location doesn't belong to object</p> <p>mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out</p> <p>segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn't contain this segment</p> <p>no_parent: Container object is deleted, but object segment was left out and not deleted</p> |
| CTIM | Tiempo de creación de fragmentos | Hora en que se creó el fragmento filtrado. |
| UUID | Identificador único universal | Identificador del objeto al que pertenece el fragmento. |
| CBID | Identificador de bloque de contenido | CBID del objeto al que pertenece el fragmento filtrado. |
| CSIZ | Tamaño de contenido | Tamaño del fragmento en bytes. |

LLST: Ubicación perdida

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

| Codificación | Campo | Descripción |
|--------------|-----------------------------|--|
| CBIL | CBID | El CBID afectado. |
| EPR | Perfil de código de borrado | Para datos de objetos codificados mediante borrado. El ID del perfil de código de borrado utilizado. |

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

MGAU: Mensaje de auditoría de gestión

La categoría Management registra las solicitudes de usuario a la API de gestión. Cada solicitud HTTP que no es una solicitud GET o HEAD a un URI de API válido registra una respuesta que contiene el nombre de usuario, la IP y el tipo de solicitud a la API. No se registran URI de API no válidos (como /api/v3-authorization) y las solicitudes no válidas a URI de API válidos.

| Codificación | Campo | Descripción |
|--------------|-------------------------|---|
| MDIP | Dirección IP de destino | La dirección IP del servidor (destino). |
| ADN MADN | Nombre de dominio | El nombre de dominio del host. |
| MPAT | RTA de la solicitud | La ruta de la solicitud. |

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

OLST: El sistema detectó un objeto perdido

Este mensaje se genera cuando el servicio DDS no puede localizar ninguna copia de un objeto dentro del sistema StorageGRID.

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

ORLM: Se cumplen las reglas de objeto

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



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

| Codificación | Campo | Descripción |
|--------------|--------------------------------------|---|
| BUID | Cabezal del cucharón | Campo ID de bloque. Se usa para operaciones internas. Sólo aparece si STAT es PRGD. |
| CBID | Identificador de bloque de contenido | El CBID del objeto. |
| CSIZ | Tamaño de contenido | El tamaño del objeto en bytes. |

| Codificación | Campo | Descripción |
|------------------------|-------------------------------|---|
| BLOQUEOS | Ubicaciones | <p>La ubicación de almacenamiento de los datos del objeto dentro del sistema StorageGRID. El valor para LOCS es "" si el objeto no tiene ubicaciones (por ejemplo, se ha eliminado).</p> <p>CLEC: Para los objetos con código de borrado, el ID de perfil de codificación de borrado y el ID de grupo de codificación de borrado que se aplica a los datos del objeto.</p> <p>CLDI: Para los objetos replicados, el ID de nodo LDR y el ID de volumen de la ubicación del objeto.</p> <p>CLNL: ID de nodo DE ARCO de la ubicación del objeto si se archivan los datos del objeto.</p> |
| RUTA | S3 Cubo/llave | El nombre del cubo S3 y el nombre de la clave S3. |
| TRANSFORMACIÓN DIGITAL | Resultado | <p>Resultado de la operación de ILM.</p> <p>SUCS: La operación de ILM fue exitosa.</p> |
| REGLA | Etiqueta de reglas | La etiqueta legible para seres humanos proporcionada a la regla ILM aplicada a este objeto. |
| SEGC | UUID del contenedor | UUID del contenedor del objeto segmentado. Este valor sólo está disponible si el objeto está segmentado. |
| SGCB | CBID del contenedor | CBID del contenedor del objeto segmentado. Este valor sólo está disponible para objetos segmentados y multipartes. |
| URGENTE | Estado | <p>El estado de la operación de ILM.</p> <p>DONE: Se completaron las operaciones de ILM contra el objeto.</p> <p>DFER: El objeto se ha marcado para una futura reevaluación de ILM.</p> <p>PRGD: El objeto se ha eliminado del sistema StorageGRID.</p> <p>NLOC: Los datos del objeto ya no se pueden encontrar en el sistema StorageGRID. Este estado podría indicar que todas las copias de los datos del objeto faltan o están dañadas.</p> |
| UUID | Identificador único universal | El identificador del objeto dentro del sistema StorageGRID. |
| VSID | ID de versión | El código de versión de un nuevo objeto creado en un bloque con versiones. Las operaciones en cubos y objetos en depósitos sin versiones no incluyen este campo. |

El mensaje de auditoría ORLM se puede emitir más de una vez para un solo objeto. Por ejemplo, se emite

cada vez que ocurre uno de los siguientes eventos:

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

Información relacionada

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

OVWR: Sobrescritura de objetos

Este mensaje se genera cuando una operación externa (solicitada por el cliente) hace que un objeto sea sobrescrito por otro objeto.

| Codificación | Campo | Descripción |
|------------------------|---|--|
| CBID | Identificador de bloque de contenido (nuevo) | CBID para el nuevo objeto. |
| CSIZ | Tamaño de objeto anterior | El tamaño, en bytes, del objeto que se sobrescribe. |
| OCBD | Identificador de bloque de contenido (anterior) | El CBID del objeto anterior. |
| UUID | ID único universal (nuevo) | El identificador del nuevo objeto dentro del sistema StorageGRID. |
| OUID | ID único universal (anterior) | El identificador del objeto anterior dentro del sistema StorageGRID. |
| RUTA | Ruta de objeto S3 | La ruta de acceso del objeto S3 utilizada tanto para el objeto anterior como para el nuevo |
| TRANSFORMACIÓN DIGITAL | Código de resultado | Resultado de la transacción de sobrescritura de objetos. El resultado es siempre: SUCS: Exitoso |

| Codificación | Campo | Descripción |
|--------------|----------------|---|
| SGRP | Planta (grupo) | Si está presente, el objeto sobreescrito se eliminó en el sitio especificado, que no es el sitio donde se ingirió el objeto sobreescrito. |

S3SL: S3 Seleccione la solicitud

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

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

| Codificación | Campo | Descripción |
|--------------|---|---|
| S3BK | S3 cucharón | El nombre de bloque de S3. |
| S3AK | ID de clave de acceso S3 (remitente de solicitudes) | El ID de clave de acceso S3 para el usuario que envió la solicitud. |
| S3AI | ID de cuenta de inquilino de S3 (remitente de solicitud) | El ID de cuenta de inquilino del usuario que envió la solicitud. |
| S3KY | Clave de S3 | El nombre de clave S3, sin incluir el nombre del bloque. |

SADD: Desactivación de auditoría de seguridad

Este mensaje indica que el servicio de origen (ID de nodo) ha desactivado el registro de mensajes de auditoría; los mensajes de auditoría ya no se recopilan ni se entregan.

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

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

SADE: Activación de auditoría de seguridad

Este mensaje indica que el servicio de origen (ID de nodo) ha restaurado el registro de mensajes de auditoría; los mensajes de auditoría se vuelven a recopilar y entregar.

| Codificación | Campo | Descripción |
|--------------|-------------------|---|
| AETM | Activar método | Método utilizado para activar la auditoría. |
| AEUN | Nombre de usuario | Nombre de usuario que ejecutó el comando para habilitar el registro de auditoría. |

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

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

SCMT: Confirmación del almacén de objetos

El contenido de la cuadrícula no está disponible ni se reconoce como almacenado hasta que se ha cometido (lo que significa que se ha almacenado de forma persistente). El contenido almacenado de forma persistente se ha escrito completamente en el disco y ha pasado las comprobaciones de integridad relacionadas. Este mensaje se genera cuando un bloque de contenido se confirma en el almacenamiento.

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

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

SDEL: ELIMINACIÓN DE S3

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

| Codificación | Campo | Descripción |
|--------------|---------------------------------------|---|
| CBID | Identificador de bloque de contenido | Identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0. Las operaciones en los depósitos no incluyen este campo. |
| CNCH | Encabezado de control de consistencia | El valor del encabezado de solicitud HTTP de control de coherencia, si está presente en la solicitud. |

| Codificación | Campo | Descripción |
|------------------------|--|---|
| CNID | Identificador de conexión | Identificador único del sistema para la conexión TCP/IP. |
| CSIZ | Tamaño de contenido | El tamaño del objeto eliminado en bytes. Las operaciones en los depósitos no incluyen este campo. |
| DMRK | Eliminar ID de versión del marcador | El código de versión del marcador de borrado creado al eliminar un objeto de un bloque con versiones. Las operaciones en los depósitos no incluyen este campo. |
| GFID | ID de conexión de federación de grid | El ID de conexión de la conexión de federación de grid asociada con una solicitud de eliminación de replicación entre grid. Solo se incluyen en los registros de auditoría en el grid de destino. |
| GFSA | ID de cuenta de origen de federación de grid | El ID de cuenta del inquilino en la cuadrícula de origen para una solicitud de eliminación de replicación entre grid. Solo se incluyen en los registros de auditoría en el grid de destino. |
| HTRH | Encabezado de solicitud HTTP | <p>Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>`X-Forwarded-For` Se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p> <p>x-amz-bypass-governance-retention se incluye automáticamente si está presente en la solicitud.</p> </div> |
| MTME | Hora de la última modificación | La Marca de hora de Unix, en microsegundos, indica cuándo se modificó por última vez el objeto. |
| TRANSFORMACIÓN DIGITAL | Código de resultado | Resultado de la transacción DE ELIMINACIÓN. El resultado es siempre: SUCS: Exitoso |
| S3AI | ID de cuenta de inquilino de S3 (remitente de solicitud) | El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo. |

| Codificación | Campo | Descripción |
|--------------|---|---|
| S3AK | ID de clave de acceso S3 (remitente de solicitudes) | El ID de clave de acceso de S3 hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo. |
| S3BK | Bloque de S3 | El nombre de bloque de S3. |
| S3KY | Clave de S3 | El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo. |
| S3SR | Subrecurso de S3 | El bloque o subrecurso de objeto en el que se opera, si procede. |
| SACC | Nombre de cuenta de inquilino de S3 (remitente de la solicitud) | El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas. |
| SAIP | Dirección IP (remitente de solicitud) | La dirección IP de la aplicación cliente que realizó la solicitud. |
| SBAC | Nombre de cuenta de inquilino de S3 (propietario del bloque) | El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo. |
| SBAI | ID de cuenta de inquilino de S3 (propietario del bloque) | El ID de cuenta de inquilino del propietario del bloque de destino. Se utiliza para identificar el acceso de cuenta cruzada o anónimo. |
| SGRP | Planta (grupo) | Si está presente, el objeto se eliminó en el sitio especificado, que no es el sitio donde se ingirió el objeto. |
| SUSR | URN de usuario de S3 (remitente de solicitudes) | El ID de cuenta de arrendatario y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vacío para solicitudes anónimas. |
| TIEMPO | Tiempo | Tiempo de procesamiento total de la solicitud en microsegundos. |

| Codificación | Campo | Descripción |
|--------------|---|--|
| TLIP | Dirección IP del equilibrador de carga de confianza | Si la solicitud se enrutó por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga. |
| UUDM | Identificador único universal para un marcador de supresión | Identificador de un marcador de borrado. Los mensajes de registro de auditoría especifican UDM o UUID, donde UUDM indica un marcador de supresión creado como resultado de una solicitud de supresión de objeto y UUID indica un objeto. |
| UUID | Identificador único universal | El identificador del objeto dentro del sistema StorageGRID. |
| VSID | ID de versión | El código de versión de la versión específica de un objeto que se eliminó. Las operaciones en cubos y objetos en depósitos sin versiones no incluyen este campo. |

SGET: S3 GET

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

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

| Codificación | Campo | Descripción |
|------------------------|--|--|
| HTRH | Encabezado de solicitud HTTP | <p>Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>`X-Forwarded-For` Se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p> </div> |
| MENIDAD | ListObjectsV2 | Se solicitó una respuesta <i>v2 format</i> . Para obtener más información, consulte " AWS ListObjectsV2 ". Sólo para OPERACIONES de OBTENCIÓN DE cucharón. |
| NCHD | Número de hijos | Incluye claves y prefijos comunes. Sólo para OPERACIONES de OBTENCIÓN DE cucharón. |
| SONÓ | Lectura de rango | Solo para operaciones de lectura de rango. Indica el rango de bytes que se ha leído en esta solicitud. El valor después de la barra inclinada (/) muestra el tamaño de todo el objeto. |
| TRANSFORMACIÓN DIGITAL | Código de resultado | Resultado DE LA transacción GET. El resultado es siempre: SUCS: Exitoso |
| S3AI | ID de cuenta de inquilino de S3 (remitente de solicitud) | El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo. |
| S3AK | ID de clave de acceso S3 (remitente de solicitudes) | El ID de clave de acceso de S3 hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo. |
| S3BK | Bloque de S3 | El nombre de bloque de S3. |
| S3KY | Clave de S3 | El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo. |
| S3SR | Subrecurso de S3 | El bloque o subrecurso de objeto en el que se opera, si procede. |

| Codificación | Campo | Descripción |
|--------------|---|--|
| SACC | Nombre de cuenta de inquilino de S3 (remitente de la solicitud) | El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas. |
| SAIP | Dirección IP (remitente de solicitud) | La dirección IP de la aplicación cliente que realizó la solicitud. |
| SBAC | Nombre de cuenta de inquilino de S3 (propietario del bloque) | El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo. |
| SBAI | ID de cuenta de inquilino de S3 (propietario del bloque) | El ID de cuenta de inquilino del propietario del bloque de destino. Se utiliza para identificar el acceso de cuenta cruzada o anónimo. |
| SUSR | URN de usuario de S3 (remitente de solicitudes) | El ID de cuenta de arrendatario y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: urn:sgws:identity::03393893651506583485:root Vacío para solicitudes anónimas. |
| TIEMPO | Tiempo | Tiempo de procesamiento total de la solicitud en microsegundos. |
| TLIP | Dirección IP del equilibrador de carga de confianza | Si la solicitud se enrutó por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga. |
| TRNC | Truncado o no truncado | Si se devuelven todos los resultados, se establece en false. Establezca como verdadero si hay más resultados disponibles para devolver. Sólo para OPERACIONES de OBTENCIÓN DE cucharón. |
| UUID | Identificador único universal | El identificador del objeto dentro del sistema StorageGRID. |
| VSID | ID de versión | El código de versión de la versión específica de un objeto que se solicitó. Las operaciones en cubos y objetos en depósitos sin versiones no incluyen este campo. |

SHEA: CABEZA S3

Cuando un cliente S3 emite una operación HEAD, se realiza una solicitud para verificar la existencia de un objeto o depósito y recuperar los metadatos sobre un objeto. El servidor emite este mensaje si la operación es exitosa.

| Codificación | Campo | Descripción |
|------------------------|--|---|
| CBID | Identificador de bloque de contenido | Identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0. Las operaciones en los depósitos no incluyen este campo. |
| CNID | Identificador de conexión | Identificador único del sistema para la conexión TCP/IP. |
| CSIZ | Tamaño de contenido | El tamaño del objeto verificado en bytes. Las operaciones en los depósitos no incluyen este campo. |
| HTRH | Encabezado de solicitud HTTP | <p>Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración.</p> <p>`X-Forwarded-For` Se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p> |
| TRANSFORMACIÓN DIGITAL | Código de resultado | Resultado DE LA transacción GET. El resultado es siempre: SUCS: Exitoso |
| S3AI | ID de cuenta de inquilino de S3 (remitente de solicitud) | El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo. |
| S3AK | ID de clave de acceso S3 (remitente de solicitudes) | El ID de clave de acceso de S3 hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo. |
| S3BK | Bloque de S3 | El nombre de bloque de S3. |
| S3KY | Clave de S3 | El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo. |

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

SPOS: PUBLICACIÓN DE S3

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

| Codificación | Campo | Descripción |
|------------------------|--|---|
| CBID | Identificador de bloque de contenido | Identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0. |
| CNCH | Encabezado de control de consistencia | El valor del encabezado de solicitud HTTP de control de coherencia, si está presente en la solicitud. |
| CNID | Identificador de conexión | Identificador único del sistema para la conexión TCP/IP. |
| CSIZ | Tamaño de contenido | El tamaño del objeto recuperado en bytes. |
| HTRH | Encabezado de solicitud HTTP | <p>Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración.</p> <p style="border: 1px solid black; padding: 5px;">`X-Forwarded-For` Se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p> <p>(No se espera para SPOS).</p> |
| TRANSFORMACIÓN DIGITAL | Código de resultado | Resultado de la solicitud RestoreObject. El resultado es siempre: SUCS: Exitoso |
| S3AI | ID de cuenta de inquilino de S3 (remitente de solicitud) | El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo. |
| S3AK | ID de clave de acceso S3 (remitente de solicitudes) | El ID de clave de acceso de S3 hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo. |
| S3BK | Bloque de S3 | El nombre de bloque de S3. |
| S3KY | Clave de S3 | El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo. |

| Codificación | Campo | Descripción |
|--------------|---|---|
| S3SR | Subrecurso de S3 | El bloque o subrecurso de objeto en el que se opera, si procede. Establezca en SELECT para una operación S3 Select. |
| SACC | Nombre de cuenta de inquilino de S3 (remitente de la solicitud) | El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas. |
| SAIP | Dirección IP (remitente de solicitud) | La dirección IP de la aplicación cliente que realizó la solicitud. |
| SBAC | Nombre de cuenta de inquilino de S3 (propietario del bloque) | El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo. |
| SBAI | ID de cuenta de inquilino de S3 (propietario del bloque) | El ID de cuenta de inquilino del propietario del bloque de destino. Se utiliza para identificar el acceso de cuenta cruzada o anónimo. |
| SRCF | Configuración del subrecurso | Restaurar información. |
| SUSR | URN de usuario de S3 (remitente de solicitudes) | El ID de cuenta de arrendatario y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vacío para solicitudes anónimas. |
| TIEMPO | Tiempo | Tiempo de procesamiento total de la solicitud en microsegundos. |
| TLIP | Dirección IP del equilibrador de carga de confianza | Si la solicitud se enrutó por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga. |
| UUID | Identificador único universal | El identificador del objeto dentro del sistema StorageGRID. |

| Codificación | Campo | Descripción |
|--------------|---------------|---|
| VSID | ID de versión | El código de versión de la versión específica de un objeto que se solicitó. Las operaciones en cubos y objetos en depósitos sin versiones no incluyen este campo. |

SPUT: S3 PUT

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

| Codificación | Campo | Descripción |
|--------------|--|--|
| CBID | Identificador de bloque de contenido | Identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0. Las operaciones en los depósitos no incluyen este campo. |
| CMPS | Configuración de cumplimiento de normativas | La configuración de cumplimiento utilizada al crear el depósito, si está presente en la solicitud (truncada a los primeros 1024 caracteres). |
| CNCH | Encabezado de control de consistencia | El valor del encabezado de solicitud HTTP de control de coherencia, si está presente en la solicitud. |
| CNID | Identificador de conexión | Identificador único del sistema para la conexión TCP/IP. |
| CSIZ | Tamaño de contenido | El tamaño del objeto recuperado en bytes. Las operaciones en los depósitos no incluyen este campo. |
| GFID | ID de conexión de federación de grid | El ID de conexión de la conexión de federación de grid asociada con una solicitud PUT DE replicación entre grid. Solo se incluyen en los registros de auditoría en el grid de destino. |
| GFSA | ID de cuenta de origen de federación de grid | El ID de cuenta del inquilino en la cuadrícula de origen para una solicitud de PUT DE replicación entre grid. Solo se incluyen en los registros de auditoría en el grid de destino. |

| Codificación | Campo | Descripción |
|------------------------|--|--|
| HTRH | Encabezado de solicitud HTTP | <p>Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>`X-Forwarded-For` Se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p> </div> <p>x-amz-bypass-governance-retention se incluye automáticamente si está presente en la solicitud.</p> |
| LKEN | Bloqueo de objeto activado | Valor de la cabecera de solicitud x-amz-bucket-object-lock-enabled , si está presente en la solicitud. |
| LKLH | Bloqueo de objeto retención legal | Valor de la cabecera de solicitud x-amz-object-lock-legal-hold , si está presente en la solicitud PutObject. |
| LKMD | Modo de retención de bloqueo de objetos | Valor de la cabecera de solicitud x-amz-object-lock-mode , si está presente en la solicitud PutObject. |
| LKRU | Bloqueo de objeto mantener hasta la fecha | Valor de la cabecera de solicitud x-amz-object-lock-retain-until-date , si está presente en la solicitud PutObject. Los valores se limitan a dentro de los 100 años posteriores a la fecha en que se ingirió el objeto. |
| MTME | Hora de la última modificación | La Marca de hora de Unix, en microsegundos, indica cuándo se modificó por última vez el objeto. |
| TRANSFORMACIÓN DIGITAL | Código de resultado | Resultado DE LA transacción PUT. El resultado es siempre: SUCC: Exitoso |
| S3AI | ID de cuenta de inquilino de S3 (remitente de solicitud) | El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo. |
| S3AK | ID de clave de acceso S3 (remitente de solicitudes) | El ID de clave de acceso de S3 hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo. |

| Codificación | Campo | Descripción |
|--------------|---|---|
| S3BK | Bloque de S3 | El nombre de bloque de S3. |
| S3KY | Clave de S3 | El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo. |
| S3SR | Subrecurso de S3 | El bloque o subrecurso de objeto en el que se opera, si procede. |
| SACC | Nombre de cuenta de inquilino de S3 (remitente de la solicitud) | El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas. |
| SAIP | Dirección IP (remitente de solicitud) | La dirección IP de la aplicación cliente que realizó la solicitud. |
| SBAC | Nombre de cuenta de inquilino de S3 (propietario del bloque) | El nombre de cuenta de inquilino para el propietario del bloque. Se utiliza para identificar el acceso de cuenta cruzada o anónimo. |
| SBAI | ID de cuenta de inquilino de S3 (propietario del bloque) | El ID de cuenta de inquilino del propietario del bloque de destino. Se utiliza para identificar el acceso de cuenta cruzada o anónimo. |
| SRCF | Configuración del subrecurso | La nueva configuración del subrecurso (truncada a los primeros 1024 caracteres). |
| SUSR | URN de usuario de S3 (remitente de solicitudes) | El ID de cuenta de arrendatario y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vacío para solicitudes anónimas. |
| TIEMPO | Tiempo | Tiempo de procesamiento total de la solicitud en microsegundos. |
| TLIP | Dirección IP del equilibrador de carga de confianza | Si la solicitud se enrutó por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga. |

| Codificación | Campo | Descripción |
|--------------|--------------------------------|--|
| ID | ID de carga | Solo se incluye en los mensajes SPUT para las operaciones CompleteMultipartUpload. Indica que todas las piezas se han cargado y ensamblado. |
| UUID | Identificador único universal | El identificador del objeto dentro del sistema StorageGRID. |
| VSID | ID de versión | El código de versión de un nuevo objeto creado en un bloque con versiones. Las operaciones en cubos y objetos en depósitos sin versiones no incluyen este campo. |
| VSST | Estado de control de versiones | El nuevo estado de creación de versiones de un bloque. Se utilizan dos estados: "Activado" o "Suspendido". Las operaciones en objetos no incluyen este campo. |

SREM: Almacén de objetos Quitar

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

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

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

SUPD: Se han actualizado metadatos S3

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

| Codificación | Campo | Descripción |
|--------------|--------------------------------------|---|
| CBID | Identificador de bloque de contenido | Identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0. Las operaciones en los depósitos no incluyen este campo. |

| Codificación | Campo | Descripción |
|------------------------|---|---|
| CNCH | Encabezado de control de consistencia | El valor del encabezado de solicitud HTTP de control de coherencia, si está presente en la solicitud, al actualizar la configuración de cumplimiento de un bloque. |
| CNID | Identificador de conexión | Identificador único del sistema para la conexión TCP/IP. |
| CSIZ | Tamaño de contenido | El tamaño del objeto recuperado en bytes. Las operaciones en los depósitos no incluyen este campo. |
| HTRH | Encabezado de solicitud HTTP | <p>Lista de los nombres de encabezado y valores registrados de la solicitud HTTP como seleccionados durante la configuración.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>`X-Forwarded-For` Se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).</p> </div> |
| TRANSFORMACIÓN DIGITAL | Código de resultado | Resultado DE LA transacción GET. El resultado es siempre: SUCCS: Exitoso |
| S3AI | ID de cuenta de inquilino de S3 (remitente de solicitud) | El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo. |
| S3AK | ID de clave de acceso S3 (remitente de solicitudes) | El ID de clave de acceso de S3 hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo. |
| S3BK | Bloque de S3 | El nombre de bloque de S3. |
| S3KY | Clave de S3 | El nombre de clave S3, sin incluir el nombre del bloque. Las operaciones en los depósitos no incluyen este campo. |
| SACC | Nombre de cuenta de inquilino de S3 (remitente de la solicitud) | El nombre de la cuenta de arrendatario para el usuario que envió la solicitud. Vacío para solicitudes anónimas. |

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

SVRF: Fallo de verificación del almacén de objetos

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

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



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

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

SVRU: Verificación del almacén de objetos desconocida

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

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



El mensaje de auditoría SVRU: Object Store Verify Unknown debe supervisarse de cerca. Significa que se han detectado copias inesperadas de datos de objetos en el almacén de objetos. Esta situación debe investigarse inmediatamente para determinar cómo se crearon estas copias, ya que pueden indicar fallos de hardware inminentes.

SYSD: Parada del nodo

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

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

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

SYST: Nodo detenido

Cuando se detiene correctamente un servicio, este mensaje se genera para indicar que se ha solicitado el cierre y que el servicio ha iniciado su secuencia de apagado. SYST se puede utilizar para determinar si se solicitó el apagado antes de reiniciar el servicio (a diferencia de SYSD, que normalmente se envía después de que se reinicia el servicio).

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

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

SYSU: Inicio del nodo

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

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

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

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

Información de copyright

Copyright © 2026 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.